Department of Homeland Security Daily Open Source Infrastructure Report for 16 October 2006

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

Daily Highlights

- President Bush on Friday, October 13, signed a law to protect U.S. ports from terrorists smuggling weapons into the United States hidden within the 11 million containers that enter the country each year. (See item 11)
- The Federal Aviation Administration has banned fixed−wing planes from the East River corridor in New York unless the pilot is in contact with air traffic control; this will affect small aircraft, but not helicopters. (See item 12)
- Hawaii Governor Linda Lingle issued a disaster declaration for the entire state on Sunday, October 15, after a strong earthquake −− which was measured by the National Earthquake Information Center as 6.6 in magnitude −− rumbled throughout the Big Island. (See item 38)

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 12, Reuters* — **German spy boss says attacks on energy rising.** Attacks on energy facilities worldwide to hinder the delivery of gas and oil have been rising sharply, the head of Germany's foreign intelligence agency said on Thursday, October 12. "In the past few years we have registered a significant increase in terrorist attacks on energy infrastructure and we must

state that there have been qualitative changes," the head of Germany's Bundesnachrichtendienst, Ernst Uhrlau, told a conference on energy security. He said attacks on facilities used to be directed at disrupting regional energy supplies, such as those on Colombian oil pipelines, but noted this had changed. "Today, they are increasingly focused on limiting the global supply of energy," he said. "Around three years ago the world energy supply came into the crosshairs of al Qaeda, thereby defining attack options for the Islamist terrorist network." "Questions of energy security will fundamentally help determine the security agenda of the 21st century," Uhrlau said.
Source: http://www.alertnet.org/thenews/newsdesk/L12894551.htm

2. *October 12, NY 1 News (NY)* — **Con Ed releases report on Queens blackout.** Con Edison released its report on July's massive power outage in Northwest Queens Thursday, October 12. The 600−page report details the circumstances that led up to the blackout, as well as what the utility plans to do to make sure it doesn't happen again. Con Ed says a series of unprecedented events during a time of peak usage resulted in 10 of the area's 22 feeder cables shorting out. And Con Ed says the action it took at the time stopped the blackout from spreading to tens of thousands of other customers. To prevent future blackouts, Con Ed says it is planning a number of changes including upgrading its equipment within the Northern Queens substation and investing $58 million in the Long Island City network. The utility also plans to add new call centers as well as install a better system to keep track of outages.
Source: http://www.ny1.com/ny1/content/index.jsp?stid=1&aid=63411

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *October 13, U.S. Air Force* — **Tanker hits top of the charts for recapitalization priority.** The Air Force's new No. 1 procurement priority is the KC−X tanker, replacing the F−22 Raptor. Since the Air Force has secured multi−year procurement funding for the Raptor from Congress, it has shifted its procurement priorities. "Our priorities for procurement are the following: KC−X, the new tanker, is No. 1," said Chief of Staff of the Air Force General T. Michael Moseley. "CSAR−X, the new combat rescue helicopter, is No. 2. Our space−based early warning and communications satellites are No 3. The F−35 (Lightning II) is No. 4. And the next generation long range strike is No. 5."
Source: http://www.af.mil/news/story.asp?id=123029037

4. *October 13, New York Times* — **Air Force seeks $13 billion to start replacing tankers.** Air Force officials said Thursday, October 12, that they were seeking $13 billion over the next five years to replace their aging fleet of aerial refueling aircraft, a process that will take decades and could grow into one of the service's largest procurement programs. Air Force Secretary Michael W. Wynne and Gen. T. Michael Moseley, the Air Force chief of staff, said that they

hoped to award a contract by next summer and that the current timetable calls for the first planes to be delivered by 2011. General Moseley said that the Air Force intended to buy 10 to 15 planes a year, ending up with a total fleet of about 450 aircraft. Some analysts have said the cost of replacing the tankers could total more than $100 billion over the next three decades. The Pentagon will include the request for the $13 billion to begin buying the tankers in its budget proposal for the fiscal year 2008, which will be formally presented next February.
Source: http://www.nytimes.com/2006/10/13/business/13tanker.html?_r=1&adxnnl=1&oref=slogin&ref=business&adxnnlx=1160749551−seJRR 4LOoJcHfd/qOfcFqQ

[Return to top]

Banking and Finance Sector

5. *October 12, Canadian Press* — **Hackers steal personal information from Brock University computers.** The personal information −− including some credit card and bank account numbers −− of about 70,000 people who gave money to Brock University has been stolen from the school's computers by a hacker. Terry Boak, Brock's vice−president academic, said the digital intruder had the secret passwords needed to access the file listing of possibly every individual to ever donate to the university. "It wasn't just someone who hacked in by playing around with it," Boak said. He said the hacker tapped into the system on September 22 at 5:27 p.m. EDT, taking only four minutes to make off with the file containing thousands of names, birthdates, and e−mail addresses. About 90 credit card numbers and some 270 bank account details were also in the file. Boak said those people were called within 24 hours, while the remaining thousands received a letter in the mail explaining what had happened.
Source: http://www.cbc.ca/technology/story/2006/10/12/tech−brock.htm l

6. *October 12, SearchSecurity* — **Malicious Website poses as Google.** A security vendor is warning Web surfers to beware of a malicious Website that poses as a legitimate Google page. According to SurfControl, the malicious site spoofs Google's Italian Website and uses typo squatting, a technique that "mimics a legitimate looking domain and delivers a fraudulent Google page that looks identical to the original." The fraudulent site attempts to install ActiveX controls on a user's machine. In addition to browser hijacking, SurfControl said the Website installs a keylogging Trojan that monitors keystrokes and sends information to a remote location. The vendor said it has witnessed incidents where infected machines tried to send out malicious spam emails.
Source: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1223058,00.html

7. *October 12, Indiana University* — **Study: More Internet users may be taking phishing bait than thought.** A higher−than−expected percentage of Internet users are likely to fall victim to scam artists masquerading as trusted service providers, report researchers at the Indiana University School of Informatics (IU). "Designing Ethical Phishing Experiments: A Study of eBay Query Features" simulated "phishing" tactics used to elicit online information from eBay customers. Surveys by the Gartner Group report that about three percent of adult Americans are successfully targeted by phishing attacks each year, an amount that might be conservative given that many are reluctant to report they have been victimized, or may even be unaware of it. In contrast, the experiment conducted by IU researchers Markus Jakobsson and Jacob Ratkiewicz,

reports actual numbers. Their study, one of the first of its kind, reveals that phishers may be netting responses from as much as 14 percent of the targeted populations per attack. "Our goal was to determine the success rates of different types of phishing attacks, not only the types used today, but those that don't yet occur in the wild, too," said Jakobsson, associate professor of informatics.
Study: http://www.informatics.indiana.edu/markus/papers/ethical_phishing−jakobsson_ratkiewicz_06.pdf.
Source: http://newsinfo.iu.edu/news/page/normal/4216.html

8. *October 12, IT Pro (UK)* — **Phishing moves to SMS.** Phishing attacks on mobile phone users are a growing threat which operators must take immediate steps to prevent, says consulting firm LogicaCMG. SMS phishing, sometimes shortened to smishing, uses text messages to trick users into handing over valuable private information or go to fake Websites where spyware and other malicious programs can be downloaded, says LogicaCMG Telecom's Chris Newton−Smith. He says mobile operators have a big role to play in protecting consumer and business users from falling victim to smishing scams. "People are using these malicious spams for social engineering −− encouraging people to ring a false customer care hotline which costs an astronomical amount per minute." He says some mobile operators have been slow to react to the issue. "Some are attaching warnings to messages that come from outside the network, so it's not necessarily just a matter of blocking," he says. But mobile and wireless analyst Mike Hijdra of 2Fast4Wireless believes the problem is actually fairly small. A bigger threat, he believes, comes from malicious attacks via Bluetooth wireless technology. "SMS is monitored, but Bluetooth is point to point so much more open to attack," he warned.
Source: http://www.itpro.co.uk/news/95530/phishing−moves−to−sms.html

9. *October 11, Mail Tribune (OR)* — **ID theft scam spurs fraud alert.** The Jackson County, FL Sheriff's Department has issued a warning about an identity theft scheme in which people claiming to work for the federal court system demand personal information. A fraud alert prepared by sheriff's Detective Sgt. Colin Fagan warns that the callers identify themselves as U.S. court employees, then tell people that they have been selected for jury duty or that a warrant has been issued for their arrest because they failed to appear for jury duty. The callers ask people to verify names and Social Security numbers, then ask for credit card numbers. If the request is refused, the callers threaten fines or arrest. The sheriff's department got about half a dozen reports of the scam last month and suspects that other people also received the suspicious calls. The fraud alert was first sent out through a network of law enforcement and financial institutions called the Southern Oregon Fraud and Security Team, or SO−FAST, that proactively coordinates information on scams, schemes and robberies.
Source: http://www.mailtribune.com/archive/2006/1011/local/stories/s cams_10−11.htm

[Return to top]

Transportation and Border Security Sector

10. *October 15, Associated Press* — **TSA screener faces theft charge.** A screener with the Transportation Security Administration was arrested after a passenger reported that she took money from the passenger's wallet. The screener, a 26−year−old woman, was taken to jail Saturday, October 14, awaiting a charge of theft and was being held on $200 bail, according to

the Milwaukee County Sheriff's Department. The passenger was waiting to go through screening at General Mitchell International Airport in Milwaukee when the incident occurred, sheriff's officials said. The passenger reported losing $20. But officials eventually recovered $235 after the screener's co−worker told authorities he saw her storing items behind a magazine rack.
Source: http://hosted.ap.org/dynamic/stories/B/BRF_TSA_THEFT_ALLEGATIONS?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

11. *October 14, Washington Times* — **Bush signs bill on port safety.** President Bush on Friday, October 13, signed a law to protect U.S. ports from terrorists smuggling weapons into the United States hidden within the 11 million containers that enter the country each year. The SAFE act authorizes $3.4 billion over five years for safety measures, including the installation of radiation detectors at the 22 largest U.S. ports by the end of next year. More inspectors will be hired to increase the number of random searches of containers. The bill was approved on a 409−2 vote in the House, and by a voice vote in the Senate.
Source: http://www.washtimes.com/national/20061013−114718−4934r.htm

12. *October 13, Associated Press* — **FAA restricts Manhattan flight path.** Fixed−wing planes have been banned from the East River corridor in New York unless the pilot is in contact with air traffic control, the Federal Aviation Administration (FAA) said Friday, October 13. The announcement comes two days after a plane carrying New York Yankees pitcher Cory Lidle above the East River slammed into a skyscraper. The new ban will affect small aircraft, but not helicopters, that previously have been allowed to fly along the river, which runs along the east side of Manhattan Island. All air traffic along the river has been limited to 1,100 feet in altitude. The FAA said a review of operations and procedures in the East River corridor prompted the rule change, which will require pilots of small, fixed−wing aircraft to obtain approval from air traffic controllers before entering the area. The FAA said the flight restrictions go into effect immediately. New York Governor George Pataki and Senator Charles Schumer, (D−NY), had asked the FAA to require anyone flying near Manhattan to be under the supervision of air traffic controllers. "A smart terrorist could load up a small, little plane with biological, chemical or even nuclear material and fly up the Hudson or East rivers, no questions asked," said Schumer.
Source: http://www.cnn.com/2006/TRAVEL/10/13/faa.plane.crash.ap/inde x.html

13. *October 13, Associated Press* — **Jet overruns Burbank runway.** A private jet, carrying Yankees third baseman Alex Rodriguez and six others, overran a runway at Bob Hope Airport on Friday, October 13, and was brought to a halt by an arresting system. None of the seven people aboard were injured, federal officials said. The Gulfstream G−II carried five passengers and two crewmembers, the National Transportation Safety Board said in a statement from Washington, DC. It had departed from Las Vegas earlier in the day. The twin−engine jet was stopped by the Engineered Materials Arresting System, a 200−foot−long stretch of pavement injected with air bubbles designed to collapse under the weight of an aircraft as large as a Boeing 737 jet traveling as fast as 50 knots, airport spokesperson Victor Gill said.
Source: http://sportsillustrated.cnn.com/2006/baseball/mlb/10/13/arod.runway.overrun.ap/index.html

14.

October 11, Associated Press — **Thirty found in fake Border Patrol vehicle.** Thirty illegal entrants were found in a vehicle that had been made up to look like a U.S. Border Patrol transport van, authorities said. The vehicle was seized Wednesday, October 11, near San Miguel on the Tohono O'odham Indian Reservation about 70 miles southwest of Tucson, AZ. The van had horizontal green stripes along the sides, Border Patrol emblems on its doors and the words "Border Patrol" written across the rear. Border Patrol agents assigned to the Casa Grande station came in contact with the van while responding to activity in the area. After seeing the agents, the driver turned the van around and tried to return to Mexico. Authorities said the male driver abandoned the van about 100 yards from the border and sprinted into Mexico, leaving behind the 30 illegal immigrants. All 30 were taken to the law−enforcement center on the reservation and processed for illegally entering the United States.
Source: http://www.azcentral.com/news/articles/1011az−bogus−border11 −ON.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

15. *October 14, Reuters* — **Bird flu in Ohio wild birds.** Northern pintail birds in Ohio have tested positive for a low−pathogenic strain of the H5N1 bird flu virus, the U.S. government said on Saturday, October 14, adding to recent cases in Pennsylvania, Maryland and Michigan. A strain of the H5N1 avian influenza virus was found in "apparently healthy" wild birds sampled October 8 in Ottawa County, located on Lake Erie about 15 miles southeast of Toledo, the departments of Agriculture and Interior said. The government said it was conducting additional tests to determine, in part, if the ducks had H5N1 or two separate strains with one virus contributing H5 and the other N1.
Source: http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyid=2006−10−15T000750Z_01_N05265390_RTRUKOC_0_US−BIRDFLU−USA.xml&src=rss&rpc=22

16. *October 13, Associated Press* — **Chronic wasting disease found in animals.** Researchers in Wyoming have found chronic wasting disease (CWD) in the heart muscle tissue of infected white−tailed deer and elk, the University of Wyoming has announced. Researchers say the discovery marks the first time that the disease has been found in the heart tissue. The discovery is important because some hunters eat meat from the heart of animals they kill. The U.S. Centers for Disease Control and Prevention and the World Health Organization recommend against eating any animals that test positive for CWD. However, other officials also say there's no scientific evidence that humans can contract the disease from eating infected animals. Terry Kreeger, wildlife veterinarian with the Wyoming Game and Fish Department, said that the tests involved captive elk and deer that were intentionally infected with CWD at research facilities in Wyoming and Colorado.
CWD information: http://www.cwd−info.org/

Source: http://seattlepi.nwsource.com/health/1500AP_Chronic_Wasting_Disease.html

17. *October 13, Agence France−Presse* — **Dutch ease sheep disease restrictions but new infections keep turning up.** The Dutch authorities reported a growing number of cases of bluetongue disease, which is deadly for sheep, but simultaneously announced they would ease cattle transport restrictions because they were ineffective. The agriculture ministry also said it would enlarge two of the three security zones in place in the southern part of the country to encompass recently infected farms. In total 206 farms are now infected. Last week the ministry said there were 124 farms infected with bluetongue disease contained in the security zones. Several restrictions have been eased which means that farmers no longer have to keep their animals indoors at night time and animals can now be transported freely from one security zone to another.
Bluetongue information: http://www.fao.org/AG/againfo/subjects/en/health/diseases−cards/bluetongue.html
Source: http://news.yahoo.com/s/afp/20061013/hl_afp/netherlandsfarmhealth_061013161400;_ylt=ArUCdqYx.I8ntJsjl3UH3miJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

18. *October 13, Stop Soybean Rust News* — **First rust ever in Illinois.** Asian soybean rust has reached the state of Illinois for the first time ever, found in Pope County in southern Illinois. It's the tenth state with rust this year. On top of several rust finds in other states Thursday, October 12, and Friday, October 13, the discovery brings the U.S. total to 120 rust−positive counties and parishes in 10 states, with 98 of those finds on soybeans. Pope County is near rust−infected counties in eastern Kentucky, and just a bit south of the northernmost rust county, Union County, KY.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=981

[Return to top]

Food Sector

19. *October 13, New York Times* — **Source of E. coli is found.** Cattle manure collected from a California ranch under investigation by federal and state authorities contains the same strain of E. coli that killed three people and sickened nearly 200 in a recent outbreak linked to tainted spinach, federal and state food safety officials said Thursday, October 12. But while the discovery of the match between E. coli in the manure and in the tainted spinach is an unprecedented development in the scientific investigation of food−borne illnesses it does not solve the mystery of how the spinach was contaminated in the first place. Pinpointing how the bacteria made its way into the spinach fields, whether from tainted irrigation water, flooding, poor hygiene among field workers or by wildlife capable of breaking through fences, is the next challenge for investigators.
Source: http://www.nytimes.com/2006/10/13/us/13spinach.html?_r=1&hp&ex=1160712000&en=5ba6de4112816ac2&ei=5094&partner=homepage&o ref=slogin

20. *October 12, Food Safety and Inspection Service* — **Pork products recalled.** Herman Falter Packing Co., a Columbus, OH, firm, is voluntarily recalling approximately 1,178 pounds of

various pork products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Thursday, October 12. The pork products were distributed to retail and wholesale establishments in the Columbus, OH, region. The problem was discovered through FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_030_2006_Relea se/index.asp

[Return to top]

Water Sector

21. *October 12, Wisconsin State Journal* — **City well water untreated.** Madison, WI, Mayor Dave Cieslewicz has ordered an investigation into why drinking water untreated for contaminants such as bacteria flowed from a city well for 38 days without being discovered by the Madison Water Utility. No illnesses have been linked to the water, according to officials. Despite utility workers making daily checks on the well, the failure of a system that pumps chlorine and fluoride into the drinking water remained undetected, said David Denig−Chakroff, the utility's general manager. As required by law, the utility conducts daily testing for bacteria at several locations throughout the city. Tom Stunkard, who oversees regulation of the water utility for the state Department of Natural Resources, said a review of those test results from the period in question revealed no detection of microbial contamination. Denig−Chakroff said the problem was likely due to a meter that failed. The equipment that adds chlorine and fluoride to the water is dependent on a signal from the meter and with the meter broken, the signal never came.
Source: http://www.madison.com/wsj/mad/top/index.php?ntid=102842&ntp id=2

[Return to top]

Public Health Sector

22. *October 15, Associated Press* — **Indonesian bird flu toll now 53.** An 11−year−old Indonesian boy has died of the H5N1 strain of bird flu, raising the national death toll from the disease to 53, the director of the hospital where the patient was being treated said Sunday, October 15. The boy was admitted to the Sulianti Saroso Hospital for Infectious Diseases on Thursday, October 12, and died Saturday, October 14. Experts say Indonesians will continue to die until the nation stops the rampant spread of infection among its hundreds of millions of backyard poultry.
Source: http://edition.cnn.com/2006/HEALTH/conditions/10/15/indonesi a.birdflu.ap/

23. *October 13, New York Times* — **Nigeria and India cited in rise of polio cases.** Public health experts charged with overseeing the global effort to eradicate polio sought Thursday, October 12, to shine a spotlight on the handful of countries that are still persistently failing to immunize every child, particularly Nigeria and India. Campaigns to eliminate the crippling disease in those countries have suffered serious setbacks over the past year. In Nigeria, the epicenter of the disease in Africa, the number of children newly paralyzed by polio has doubled since last

year. In India, which experts had hoped could stop the disease in its tracks this year, fresh outbreaks have driven the number of new cases 10 times higher than last year. The vast majority of the 1,403 cases of polio registered so far this year have occurred in those two countries. Experts who provide independent oversight of the polio eradication effort said in interviews and a telephone news conference that strong political leadership is needed in the four countries where polio is still endemic: Nigeria, India, Pakistan and Afghanistan. Such failures are often at the state and local level. Over the past three years, people from India or Nigeria have spread the infection to 25 formerly polio−free nations.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.nytimes.com/2006/10/13/world/13polio.html

24. *October 13, Associated Press* — **Probe links 21 deaths to cough syrup.** U.S. health officials have cracked the case of what caused the mysterious deaths of 21 people in Panama since midsummer −− an industrial chemical in red cough syrup. Officials continue to investigate how the medicine became contaminated. The Panamanian government has ordered the syrup removed from store shelves and the government factory that manufactured it shut down. But U.S. health officials are tentatively counting the investigation as a success story in rapid investigation and international collaboration that may have prevented additional deaths. Many of the victims suffered kidney failure, paralysis and sagging of the facial muscles and other symptoms. Panama's Ministry of Health asked the U.S. Centers for Disease Control and Prevention (CDC) to send help. By that point more than a dozen deaths had been reported. Early Wednesday, October 11, CDC investigators found diethylene glycol in four white plastic cough syrup bottles flown in from Panama City. Diethylene glycol is a chemical cousin of antifreeze and is used to keep products like glue and cosmetics moist.
Source: http://www.breitbart.com/news/2006/10/13/D8KO24JO0.html

25. *October 13, Reuters* — **Plague confirmed in Congo, 42 reported dead.** An outbreak of plague has been confirmed in the Democratic Republic of Congo, with 42 deaths reported among 626 suspected cases over the past 10 weeks, the World Health Organization (WHO) said on Friday, October 13. But the WHO said the number of suspected cases "may be an overestimation" as the fatality ratio was unusually low for pneumonic plague. "Preliminary results from a rapid diagnosis test in the field found three samples positive, out of eight," the WHO said, confirming the presence of the disease. It said additional tests were under way. Highly contagious pneumonic plague is the most deadly form of plague. It can be spread by humans and usually kills half of its victims.
Source: http://today.reuters.com/news/articlenews.aspx?type=worldNews&storyID=2006−10−13T154332Z_01_L13117215_RTRUKOC_0_US−CONGO−DEMOCRATIC−PLAGUE.xml&WTmodLoc=IntNewsHome_C2_worldNews−8

26. *October 12, Reuters* — **New test identifies mystery New York viruses.** A quick new genetic test has helped identify mysterious germs that sickened dozens of New Yorkers in a 2004 outbreak, researchers reported on Thursday, October 12. The test may help doctors and scientists nail down the causes of outbreaks of respiratory disease, which goes unidentified in about half of all cases now. They found nine previously undiagnosed germs −− six viruses and three bacteria. About 30 percent of the patients had some type of rhinovirus, a family known for causing the common cold and other upper respiratory infections, Ian Lipkin of Columbia University and colleagues found. Eight of the specimens tested positive for rhinoviruses that are

unlike any known rhinovirus. They used a new fast, sensitive and inexpensive diagnostic tool called MassTag PCR. PCR is a technique that can quickly amplify genetic material such as DNA so it can be measured.
Abstract: http://www.journals.uchicago.edu/JID/journal/issues/v194n10/37034/brief/37034.abstract.html
Source: http://today.reuters.com/news/articlenews.aspx?type=healthNews&storyID=2006-10-12T221201Z_01_N12302645_RTRUKOC_0_US-VIRUS.xml&WTmodLoc=NewsHome-C3-healthNews-2

[Return to top]

Government Sector

27. *October 14, Associated Press* — **Teaching kids to fight back against classroom invaders.** Youngsters in Burleson, TX, school district, a suburb of Fort Worth, are being taught not to sit there like good boys and girls with their hands folded if a gunman invades the classroom, but to rush him and hit him with everything they've got -- books, pencils, legs and arms. "Getting under desks and praying for rescue from professionals is not a recipe for success," said Robin Browne, a major in the British Army reserve and an instructor for Response Options, the company providing the training to the Burleson schools. That kind of fight-back advice is all but unheard of among schools, and some fear it will get children killed. But school officials in Burleson said they are drawing on the lessons learned from a string of disasters such as Columbine in 1999 and the Amish schoolhouse attack in Pennsylvania last week. The school system in this working-class suburb of about 26,000 is believed to be the first in the nation to train all its teachers and students to fight back, Browne said. At Burleson -- which has 10 schools and about 8,500 students -- the training covers various emergencies, such as tornadoes, fires and situations where first aid is required.
Source: http://www.cnn.com/2006/EDUCATION/10/13/defending.the.classroom.ap/index.html

[Return to top]

Emergency Services Sector

28. *October 13, Miami Herald* — **Study: South Florida gets 'F' for evacuations.** South Florida ranked 34th among 37 major U.S. urban centers for its capacity to evacuate its population in the face of an emergency, the American Highway Users Alliance, a group that lobbies for more highways, reported Thursday, October 12. The study said only the New York, Chicago and Los Angeles urban areas fared worse than South Florida. Overall, 20 U.S. metropolitan areas with a population of one million or more -- including South Florida -- got an "F" grade. Only the Kansas City, MO, area obtained an "A" grade. But Florida's emergency management chief expressed skepticism over the study's findings. Fugate said the study assumes an extreme scenario in which an entire major urban area is evacuated, something he said was unlikely to occur even in a worst-case hurricane. He said that's because vulnerable coastal populations are moved to shelters within the counties, and building codes allow homes to withstand strong winds.

Emergency Evacuation Report:
http://www.miami.com/multimedia/miami/news/evacuation_report_card2006.pdf
Source: http://www.miami.com/mld/miamiherald/news/state/15745816.htm

29. *October 12, New York Post* — **NYPD, FDNY shared control in response to recent plane crash.** Massive, quick and coordinated −− with the New York Fire Department (FDNY) and the New York Police Department (NYPD) equally sharing control at the scene under new rules put into place after September 11, 2001. That's how Mayor Bloomberg and uniformed−services union leaders described the city's response to the plane crash on the Upper East Side. "It went perfectly according to plan," Bloomberg declared during a press conference a few hours after the crash. In 2004, the city issued new protocols −− called the Citywide Incident Management System −− that sets forth which city agency would be in charge during certain events, such as terror attacks, natural disasters and other emergencies. Those rules were put into effect during the response to the crash, which was classified as an "aviation incident." In that circumstance, both the FDNY and the NYPD share control equally under what is called a joint command. In cases of a chemical, biological or other hazardous−materials attack that is criminal or terror−related, the NYPD takes charge and leads the response.
Source: http://www.nypost.com/seven/10122006/news/regionalnews/call_it_fdnypd_regionalnews_david_seifman_____and_stephanie_gaskell.htm

30. *October 12, Sun Herald (MS)* — **Experts say hurricane season seems to be over early.** Though hurricane season is still six weeks from being officially over, it appears the Gulf Coast can breathe a collective sigh of relief, according to hurricane experts. "It looks like the season's over," said Dr. William Gray, a Colorado State University climatologist, during a presentation sponsored by the George C. Marshall Institute. Because of the unforeseen late−summer onset of El Nino conditions in the Pacific −− which allow warmer water to move east and thus deaden storm activity −− chances of another hurricane striking the U.S. are slim, according to Gray.
Source: http://www.sunherald.com/mld/sunherald/15737387.htm

[Return to top]

Information Technology and Telecommunications Sector

31. *October 13, CNET News* — **The future of malware: Trojan horses.** Some of the most dangerous cyberattacks are the least visible ones. Widespread worms, viruses or Trojan horses spammed to millions of mailboxes are typically not a grave concern anymore, security experts said at the Virus Bulletin conference Thursday, October 12. Instead, especially for organizations, targeted Trojan horses have become the nightmare scenario, they said. The stealthy attacks install keystroke−logging or screen−scraping software, and they are used for industrial espionage and other financially motivated crimes, experts said. Cybercrooks send messages to one or a few addresses at a targeted organization and attempt to trick their victim into opening the infected attachment −− typically, a Microsoft Office file that exploits a yet−to−be−patched vulnerability to drop the malicious payload. Security technology can stop common attacks, but targeted attacks fly under the radar. That's because traditional products, which scan e−mail at the network gateway or on the desktop, can't recognize the threat. Alarm bells will ring if a new attack targets thousands of people or more, but not if just a handful of e−mails laden with a new Trojan horse is sent.

Source: http://news.com.com/The+future+of+malware+Trojan+horses/2100−7349_3−6125453.html?tag=nefd.lede

32. *October 13, VNUNet* — **Web caches harboring exploit code.** Web caches used by search engines and ISPs are harboring malicious code thought to have been long−removed, according to a recent report. Security company Finjan said that the caching servers used by sites such as Google and Yahoo are holding exploit code that could be used by third parties to carry out an attack. "It is possible that storage and caching servers could unintentionally become the largest legitimate storage venue for malicious code," said Yuval Ben−Itzhak, chief technology officer at Finjan.
Finjan Trend Report October 2006: http://www.finjan.com/content.aspx?id=827
Source: http://www.vnunet.com/vnunet/news/2166385/web−caches−harbori ng−exploit

33. *October 13, Washington Post* — **Hackers stepping up pace of Microsoft exploits.** The cat−and−mouse game that Microsoft Corp. and hackers have been playing for years escalated last week, just as the software giant was addressing some of the biggest problems facing computer users. On Tuesday, October 10, the company released a record 26 security fixes for the Windows operating system and the widely used Office programs such as Word, Excel and Outlook. Thursday, October 12, hackers pounced again, posting on the Internet information about vulnerabilities in PowerPoint 2003, one of the Office programs widely used by business customers and increasingly used by students. Microsoft, whose products are the largest targets of hackers because its products are used on most computer systems, issues software updates to protect users' computers from the viruses, worms and spyware that are spread through their products via e−mail attachments and the Web. But because those patches are released on a regular schedule −− the second Tuesday of each month −− the people who expose and exploit the vulnerabilities in the programs tend to wait until a day or so after the monthly release to reveal other vulnerabilities they have discovered.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/12/AR2006101201744.html

34. *October 12, IDG News Service* — **Spamhaus case could cause ICANN crisis.** Last month, the District Court for the Northern District of Illinois ruled against anti−spam black−lister The Spamhaus Project Ltd. in a lawsuit brought by e−mail marketer e360Insight LLC. The court ordered Spamhaus to remove the company from its database of spammers and to pay $11.7 million in damages, but Spamhaus initially ignored the ruling, saying that the U.S. court had no jurisdiction over the UK−based project. On Friday, October 6, the judge issued a proposed order that told both the Spamhaus.org domain name registrar, Tucows Inc., and the Internet Corporation for Assigned Names and Numbers (ICANN) to pull the project's domain name. Though the order is only proposed and does not have the force of law, observers said they worry that any attempt by U.S. courts to exert control over ICANN could be bad for the Internet. The Marina Del Rey, California−based ICANN has come under fire in the past for lacking transparency and being U.S.−centric. "Suppose a U.S. court ordered ICANN to yank a prominent .com name belonging to a non−U.S. company," said Princeton University's Edward Felten. "Such a decision, if seen as unfair outside the U.S., could trigger a sort of constitutional crisis for the Net," he said.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004111

35. *October 12, eWeek* — **Expert: Hackers will break Vista's PatchGuard.** Alexander Czarnowski, chief executive of Avet, in Warsaw, Poland, said he believes it's inevitable that hackers will crack the controversial PatchGuard kernel anti−tampering technology within one year of the release of the final version of Windows Vista. The PatchGuard technology effectively serves as an anti−rootkit mechanism, blocking the insertion of kernel−mode stealth malware. However, hackers and security researchers have already started discussing ways to bypass the technology. A security researcher associated with the Metasploit Project has already published an Uninformed.org essay that proposes several different techniques that could be used to bypass PatchGuard. The technology is at the core of a bitter dispute between Microsoft and anti−virus vendors over access to sensitive parts of the new operating system. Symantec and McAfee argue that PatchGuard will limit their ability to integrate security software into Vista, but Microsoft insists the technology is crucial to securing the operating system. Source: http://www.eweek.com/article2/0,1895,2029031,00.asp

36. *October 11, Tech Web* — **Microsoft terminates support for Windows XP SP1.** Last Wednesday, October 11, Microsoft ended its support of Windows XP SP1 and SP1a with security updates. However, before ending support it issued patches last Tuesday for 10 vulnerabilities affecting the operating system, two of which were judged "critical." Source: http://www.techweb.com/wire/software/193200775

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	4662 (eDonkey2000), 1026 (win−rpc), 38973 (−−−), 61127 (−−−), 113 (auth), 17217 (−−−), 445 (microsoft−ds), 139 (netbios−ssn), 25 (smtp), 80 (www) 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

37. *October 14, South Florida Sun−Sentinel* — **Fast−track project on Lake Okeechobee dike may cost extra $50 million.** A new plan to reinforce Lake Okeechobee's aging dike could cost $50 million more and should be fast−tracked to finish in a few years instead of a few decades, water regulators said Thursday. The cost of acquiring more land for a revamped project to strengthen the Herbert Hoover Dike could range from $20 million to $50 million, said Carol Wehle, executive director of the South Florida Water Management District. The need to strengthen the 140−mile−long dike gained urgency in May after an engineering report, commissioned by the water district, declared the dike "poses a grave and imminent danger to the people and the environment of South Florida." Wehle said the district would push for help from the Florida Legislature to pay for the land and call on Congress to prioritize more money

for construction. The Army Corps of Engineers last week released a plan that calls for increasing the stability of the dike by enlarging a concrete wall that would be built through the middle of the earthen structure. The plan also adds berms along the outside base to help stop water that seeps through and erodes the 70−year−old levee.
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−plakeo13oct13,0,1841098.story?coll=sfla−home−headlines

[Return to top]

General Sector

38. *October 15, CNN* — **Hawaii governor declares statewide emergency.** Hawaii Governor Linda Lingle issued a disaster declaration for the entire state about four hours after a strong earthquake −− which was measured by the National Earthquake Information Center as 6.6 in magnitude −− rumbled throughout its Big Island at 7:07 a.m. (1:07 p.m. EDT) Sunday, October 15. There have been as many as 20 aftershocks, with the strongest recorded at 5.8, officials told CNN. The quake knocked out power at many homes across the island chain and caused at least one landslide on a major roadway on the island of Hawaii, known as the Big Island, according to Hawaii's KITV. Officials said a state of emergency had been declared. Emergency room ceilings collapsed and electricity went out at Kona Community Hospital on the Big Island, which began transporting seriously ill patients and nursing home patients to Hilo Medical Center said spokesperson Terry Lewis. Power was restored to Hilo on the Big Island. Power is slowly coming back on throughout Maui, the Hawaii National Guard said. Honolulu International Airport canceled departing flights but was still accepting arriving flights.
Source: http://www.cnn.com/2006/US/10/15/hawaii.quake/index.html

[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