# Department of Homeland Security Daily Open Source Infrastructure Report for 14 October 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

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

**Daily Highlights**

- A four−month ABC News investigation found security lapses at many of the little−known nuclear research reactors operating on college campuses across the country. (See item 2)
- The Associated Press reports a federal task force assembled on Thursday, October 13, in Laredo, TX, to discuss the escalating violence along the Texas−Mexico border. (See item 9)
- Reuters reports the European Commission said on Thursday, October 13, the H5N1 strain of bird flu has spread from Asia to the fringes of Europe, having been now documented in Turkey. (See item 18)



## 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 13, Palm Beach Post (FL)* — **Utility concerned about natural gas supplies.** Utility Florida Power & Light Co. (FPL) said Wednesday, October 12, it has adequate supplies of natural gas for now, but is concerned about what might happen if damage to Gulf Coast production continues into 2006. "As a company, we are concerned that this will have an impact on price and availability in the winter months," said Mayco Villafana, a spokesperson for FPL. Natural gas production in the gulf is down 60 percent from what it was before Hurricanes

Katrina and Rita slammed into the area, officials and industry experts say. FPL, which gets 37 percent of its fuel from natural gas, is trying to increase supplies and make the most of its other sources, which include nuclear, coal and purchased power, Villafana said. The utility is hoping that natural gas production is back to normal in time for December, January and February, he said.
Source: http://www.palmbeachpost.com/business/content/business/epaper/2005/10/13/a2d_naturalgas_1013.html

2. *October 12, ABC News* — **Investigation finds lapses in security at nuclear reactors.** A four−month ABC News investigation found security lapses at many of the little−known nuclear research reactors operating on 25 college campuses across the country. Among the findings: unmanned guard booths, a guard who appeared to be asleep, unlocked building doors and, in a number of cases, guided tours that provided easy access to control rooms and reactor pools that hold radioactive fuel. ABC News found none of the college reactors had metal detectors, and only two appear to have armed guards. Many of the schools permit vehicles in close proximity to the reactor buildings without inspection for explosives. A spokesperson for the Nuclear Regulatory Commission (NRC), which oversees the nation's campus research reactors, said that, based on the ABC News findings, the agency has opened an investigation into at least five of the schools. "The NRC will not hesitate to take strong enforcement action should we find a violation," said Eliot B. Brenner, director of the NRC's Office of Public Affairs. The NRC is also reviewing the adequacy of reactor security plans at other schools as a result of the investigation, Brenner said.
Source: http://abcnews.go.com/Primetime/LooseNukes/story?id=1206529& page=1

3. *October 12, Arizona Republic* — **Nuclear plant shut down for safety concerns.** The Palo Verde Nuclear Generating Station, located 50 miles west of Phoenix, AZ, was idle on Wednesday, October 12, after two of its three reactors were shut down due to safety concerns. A third unit at the nation's largest nuclear power plant was taken off line October 7 for refueling and repairs. Plant operator Arizona Public Service (APS) shut down the plant's two operating reactors late Tuesday, October 11, after it was unable to demonstrate to regulators that a key safety system would perform as designed. The problem, which involves an emergency system that cools the plant's nuclear reactors after an accident, also affects the third unit that is being refueled. "It's not that the system wouldn't operate, it's that we couldn't prove that it would," said APS spokesperson Jim McDonald. Given the situation, conditions of APS's operating permit required the units be shutdown. "There was no question they were going down," he said. McDonald was unable to say when the two units would be restarted. A restart would have to be cleared by the Nuclear Regulatory Commission and the safety issue would first have to be resolved. McDonald said the utility has ample power to serve its customers.
Source: http://www.azcentral.com/news/articles/1012paloverde−ON.html

[Return to top]

## Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

# Defense Industrial Base Sector

Nothing to report.
[Return to top]

# Banking and Finance Sector

4. *October 13, Insurance Journal* — **Theft protections for New Jersey consumers strengthened.** A New Jersey law recently passed by Governor Richard Codey allows consumers to freeze their credit files to prohibit thieves from opening accounts in their names. The security freeze prevents anyone from reviewing a consumer's files without the person's authorization. The freeze can be applied at no charge, and can be lifted for a $5 fee when a consumer applies for credit. New Jersey is the 12th state to enact such a law. The Identity Theft Protection Act also requires that businesses thoroughly destroy customer information, and that they notify customers if their sensitive information has been viewed by an unauthorized individual. In addition, the law restricts the use of Social Security numbers on mailed materials and membership cards. Gail Hillebrand, director of Consumers Union's Financial Privacy Now campaign, said "There is no single answer to fighting identity theft, but New Jersey's law offers a strong blueprint for lawmakers across the country working to protect consumers from this fast−growing form of financial crime."
   Source: http://www.insurancejournal.com/news/east/2005/10/13/60760.h tm

5. *October 13, INTERFAX* — **Fraudulent banking text messages becoming more prevalent.** Between September 30 and October 7, approximately 1,265 cases of fraud committed via short messaging service (SMS) were reported to Beijing's Municipal Public Security Bureau. The fraudulent SMS messages stated that the user had spent a certain amount of money in shopping malls and asked the user to call a specific phone number. A scammer posing as a bank representative then asked the user for her bank card number and password. Instances of theft were as high as $38,414 USD. To help prevent future thefts, Beijing banks have sent their specific SMS service numbers via e−mail or short messages to their customers. The Beijing Public Security Bureau is also warning the general public to beware of the fraudulent text messages.
   Source: http://www.interfax.cn/showfeature.asp?aid=6432

6. *October 12, SecurityFocus* — **Botnet arrests unlikely to curtail scamming.** Security experts say that the recent arrests of three men in the Netherlands who controlled a network of more than 100,000 computers that attacked corporate networks, captured sensitive and financial information, and sent bulk e−mail messages such as spam and phishing attacks, will most likely not restrain illegal activity surrounding botnets. Says Joe Stewart, senior security researcher at LURHQ, a security management company: "People making money off of it are not going to stop because someone else in a different country got arrested or because a large botnet got taken down. Hopefully, as law enforcement gets more clued in to how botnets operate, we will get a critical mass where it acts as an actual deterrent to these people." Analysts point out, however, that bot software now incorporates architecture into which criminals can plug new functionality that can be used against consumers. The Dutch suspects are alleged to have used such software.

Source: http://www.securityfocus.com/news/11344

7. *October 12, Republican−American (CT)* — **Scammers pose as Federal Trade Commission officials.** Connecticut consumers have recently been plagued with calls from scammers identifying themselves as representatives of the Federal Trade Commission's (FTC) "security verification department." The scammers informed consumers that their personal information may have been disclosed and then asked for a checking account or credit card number to verify the consumer's personal information. After the consumers provide the information, callers are asked to purchase medical insurance priced at $398. State Attorney General Richard Blumenthal said, "Falsely posing as a federal official to commit identity theft is a new low in con−artistry. No legitimate government agency or financial institution would ask for personal information over the phone." His office advises consumers to contact their financial institution to determine whether to close bank or brokerage accounts, change passwords, or have the institution monitor for fraud.
Source: http://www.rep−am.com/story.php?id=28690

8. *October 11, The Gazette (Montreal)* — **International Internet−based scam ring members begin trial.** The trial for the first 19 members of Shadowcrew −− an Internet−based identity theft and credit card fraud ring that was apprehended by justice officials a year ago in the U.S. Secret Service's Operation Firewall −− is scheduled for this month in Newark, NJ. In one year, the ring, which spanned North America, Latin America, and Europe, grossed $4.3 million in illicit profit. Investigators warn that former members of Shadowcrew who were not apprehended are continuing to pursue financial crimes through an operation similar to the one brought down. The organization, with members in each G8 nation, could easily proliferate because of advanced anonymizing software and hacker techniques. They are also recruiting a cadre of younger members, usually teenagers, dubbed "hackers for hire." A lack of resources, personnel, and cooperation from some countries in extraditing criminals who direct massive online scams against U.S. businesses compounds the problem.
Source: http://www.canada.com/technology/story.html?id=05a7ecc6−d0de−4fd3−a42b−94fadfe6cf37

[Return to top]

## Transportation and Border Security Sector

9. *October 13, Associated Press* — **Federal task force to combat border violence.** A federal task force assembled on Thursday, October 13, in Laredo, TX, to discuss the escalating violence along the Texas−Mexico border. Meanwhile, attorneys general from Mexico and the United States are meeting to discuss a border security partnership. U.S. Attorney General Alberto Gonzales and Mexican counterpart Daniel Cabeza de Vaca met in San Antonio to share ideas and establish a plan to reduce border violence. Gonzalez announced Wednesday, October 12, the establishment of the nation's 22nd Violent Crime Impact Team ordered to work out of Laredo on the Mexican border. The move frees federal funding to support the mission. It will use personnel from the Bureau of Alcohol, Tobacco, Firearms and Explosives, U.S. Marshals Service, FBI, and Drug Enforcement Administration.
Source: http://www.newschannel5.tv/News/Other/2838/Federal−task−force−to−combat−border−violence

10. *October 12, GovExec* — **Expansion of alien removal policy could create logistical headaches.** A potential expansion of the government's power to detain and remove illegal immigrants without hearings or review raises numerous policy, resource and logistical questions, according to a new report from the Congressional Research Service (CRS). Several lawmakers have recently expressed interest in broadening the use of expedited removal, which allows the government to immediately send home illegal aliens who lack proper documentation, or have committed fraud or willful misrepresentation of facts, without further hearings or review, unless the alien indicates a fear of persecution. The government can use expedited removal against illegal aliens at ports of entry and those found within 100 miles of the Southwest border. The Department of Homeland Security expanded the use of the procedure last month to include all border patrol sectors along the Southwest and Northern borders. Some say the authority should be applied to illegal aliens caught anywhere within the country, CRS noted in the report. "Whether the policy should be made mandatory and extended into the interior of the country is emerging as an issue," the report stated. The report did not draw any policy conclusions or make any recommendations.
Report: http://www.ilw.com/immigdaily/news/2005,1012−crs.pdf
Source: http://www.govexec.com/story_page.cfm?articleid=32544&dcn=to daysnews

11. *October 12, New York Times* — **Amtrak breakup advances.** The Amtrak board has approved an essential step in the Bush administration plan to break up the railroad, voting to carve out the Northeast Corridor, the tracks between Boston and Washington, as a separate division. The board voted in a meeting on September 22 to create a new subsidiary to own and manage the corridor, which includes nearly all the track that Amtrak owns. The plan, which would require action by Congress, is to transfer the corridor to a consortium including the federal government and the governments of the states in the region that would share the costs to maintain it. That would relieve Amtrak from spending billions of dollars to build and rebuild bridges, rails and electrical systems, but still let the company run its trains. The plan would also remove Amtrak from control of that sector, a condition that the railroad's senior executives say would doom high−speed long−distance service. Managers say they have to be able to give their trains priority over local traffic if they have any hope of keeping their schedules. A large majority of trains in the corridor are shorter−distance commuter trains operated by state agencies in metropolitan regions, although Amtrak trains accrue a majority of the miles traveled.
Source: http://www.nytimes.com/2005/10/13/national/13amtrak.html?pag ewanted=all

12. *October 12, Associated Press* — **United recalling pilots for expanded flight schedule.** United Airlines plans to recall about 300 pilots to meet an expected increase in flying next year as it comes out of bankruptcy, the nation's No. 2 airline said. The total represents nearly a sixth of those remaining on furlough and will add five percent to United's workforce of approximately 6,500 active pilots. Steve Forte, United's senior vice president for flight operations, said the airline is likely to exceed the planned total of 300 pilot recalls in 2006 once military leave and other factors are taken into account. United is targeting an emergence from bankruptcy on February 1, 2006, after it spent more than three years restructuring in Chapter 11.
Source: http://www.usatoday.com/travel/destinations/2005−10−12−north west−expansion_x.htm

13.

*October 12, Associated Press* — **Man arrested, charged in jet joy ride.** A man was arrested on charges of stealing a charter jet and taking it on a 350−mile joy ride from Florida to Georgia, police said Wednesday, October 12. The circumstances of the theft were not clear, but nothing threatening was found on the plane, police spokesperson Darren Moloney said. The incident "appears to be a joy ride," Moloney noted. Daniel Andrew Wolcott was charged with felony theft and misdemeanor reckless conduct, police said, adding that additional federal charges were expected. Investigators said they made the arrest after interviewing five people who said they were on the 10−passenger, $7 million Cessna Citation 7 when Wolcott flew it. The plane was found Monday, October 10, at the Gwinnett County Airport−Briscoe Field near Atlanta, police said. Wolcott has a commercial rated pilot's license but is not licensed to fly that type of plane, police said.
Source: http://www.sfgate.com/cgi−bin/article.cgi?file=/news/archive/2005/10/12/national/a114626D92.DTL

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

14. *October 13, The Sun News (SC)* — **Soybean rust detected in new area.** The rainy, cooler conditions are perfect for Phakopsora pachyrhizi and Phakopsora meibomiae, better known to farmers as soybean rust, which has invaded a field in Horry County, SC. It is the farthest north and east the invasive fungi have been found to date, said Horry County's Clemson Extension Agent Bruce Johnson, who found the rust in a soybean monitoring field he planted this season. If not treated, the fungus can reduce crop yields and damage any profit the grower may have in the crop. However, officials aren't worried the rust will damage any of Horry County's 50,000 acres of soybeans this year because the season is nearly complete and the fungus won't live through the winter here, Johnson said. “We found it so late the greatest majority of the beans are already made and it probably won't affect them significantly," said Johnson. According to the U.S. Department of Agriculture, soybean rust also was confirmed Tuesday, October 11, in Pickens County, the fifth county in South Carolina to detect the fungus this season.
Information on soybean rust: http://www.usda.gov/soybeanrust/
Source: http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/ local/12890849.htm

15. *October 12, WBAY (WI)* — **Wisconsin Department of Natural Resources resumes chronic wasting disease testing.** For the first time since 2002, deer hunters in Northeast Wisconsin are being urged to help with chronic wasting disease (CWD) testing. Department of Natural Resources (DNR) biologists are collecting deer heads this fall in 16 Northeast Wisconsin counties: Brown, Calumet, Door, Fond du Lac, Green Lake, Kewaunee, Manitowoc, Marinette, Marquette, Menominee, Oconto, Outagamie, Shawano, Waupaca, Waushara and Winnebago. The DNR plans to test deer around the state in a three−year cycle. It wants to make sure chronic wasting disease hasn't spread from where it was first discovered three years ago near Mount

Horeb in southwestern Wisconsin. While no wild deer in Northeast Wisconsin has ever tested positive for CWD, state wildlife experts say it's important Wisconsin stays vigilant to make sure the disease is controlled and not spreading.
Information about chronic wasting disease: http://www.aphis.usda.gov/vs/nahps/cwd/
Source: http://www.wbay.com/Global/story.asp?S=3971973&nav=51s7

[Return to top]

# Food Sector

16. *October 12, CIDRAP News* — **Oyster−related illness linked to warming ocean.** An outbreak of illness among cruise ship passengers in Alaska in 2004 led to the detection of disease−causing oysters about 620 miles farther north than they had ever been found before, possibly as a result of warming ocean waters. The report in last week's New England Journal of Medicine also suggests that current national standards for bacterial contamination in raw oysters may be too high, because oysters linked with the outbreak had contamination levels far below the standards. The cruise ship passengers got sick after eating raw oysters, and tests in most cases pointed to Vibrio parahaemolyticus, says the report by Joseph B. McLaughlin, MD, MPH, and colleagues from the Alaska Department of Health and Social Services and several other health agencies. The sound where the oysters were harvested was warmer at the time of the outbreak than in any of the preceding six summers. “The investigation extends by 1,000 km the northernmost documented source of oysters that caused illness due to V. parahaemolyticus," the report says. "Rising temperatures of ocean water seem to have contributed to one of the largest known outbreaks of V. parahaemolyticus in the United States," according to the report.
Abstract of “Outbreak of Vibrio parahaemolyticus Gastroenteritis Associated with Alaskan Oysters”: http://content.nejm.org/cgi/content/abstract/353/14/1463
Information about Vibrio parahaemolyticus:
http://www.cdc.gov/ncidod/dbmd/diseaseinfo/vibrioparahaemoly ticus_g.htm
Source: http://www.cidrap.umn.edu/cidrap/content/fs/food−disease/new s/oct1205vibrio.html

[Return to top]

# Water Sector

17. *October 13, South Florida Sun−Sentinel* — **Water district to give local governments millions for water projects.** South Florida water managers agreed Wednesday, October 12, to give local governments $43.1 million to develop other sources of water, largely by recycling treated sewage and tapping into underused, brackish groundwater. The bulk of that money, $30 million, comes from the state Legislature, which is pushing the program to help cities and counties look beyond easy, cheap, and heavily used supplies to find sources of additional water for population growth. In southeast Florida, the main source has long been the Biscayne Aquifer, a huge porous rock formation many utilities draw upon for drinking water. The $43.1 million the South Florida Water Management District will distribute this fiscal year is seven times the amount of financial aid for alternative water the district parceled out last fiscal year. Promoting alternative water helps reduce the risk of exhausting the region's main water supplies. It protects wetlands, too, since well fields sunk into the Biscayne Aquifer are fed by

water withdrawn at times from the Everglades, said Carlyn Kowalsky, water supply department director for the water district.
Source: http://www.sun−sentinel.com/news/local/palmbeach/sfl−pwater13oct13,0,7270241.story?coll=sfla−news−palm

[Return to top]

## Public Health Sector

18. *October 13, Reuters* — **Deadly Asian bird flu reaches fringes of Europe.** The H5N1 strain of bird flu has spread from Asia to the fringes of Europe, the European Commission (EU) said on Thursday, October 13, warning countries to prepare for a potential pandemic. EU Health and Consumer Protection chief Markos Kyprianou said a strain of bird flu found in Turkey had been identified as the same H5N1 virus that killed more than 60 people in Asia since 2003 and forced the slaughter of millions of birds. The EU's executive was also assuming that the bird flu found in Romania was the same virulent strain, he said, though further tests are needed to confirm this. The European Commission has banned imports of live birds and poultry meat from both Turkey, where it was discovered at a farm near the Aegean and Marmara seas, and Romania. Kyprianou said the European Commission was considering establishing a one billion euro "solidarity fund" to help pay for anti−virals in the event of a pandemic. EU experts on avian influenza and migratory birds will hold an emergency meeting in Brussels on Friday, October 14.
Source: http://today.reuters.com/news/NewsArticle.aspx?type=topNews&storyID=2005−10−13T124613Z_01_ROB340139_RTRUKOC_0_US−BIRDFLU .xml

19. *October 13, Cambridge Chronicle (MA)* — **Massachusetts city participates in avian flu drill.** This year, the Cambridge, MA, Public Health Department has ramped up preparedness efforts for a potential flu pandemic. The Health Department participated in a drill on Thursday, September 29, in which public health officials, hospital and emergency medical technician staff, police, firefighters and civic leaders from nine communities worked collaboratively to respond to an avian flu outbreak. In this fictional scenario, a man arrived at a Boston area hospital with flu−like symptoms. The man had recently returned from a business trip to Asia, and had potentially infected several hundred passengers on his flight home. During the training, Massachusetts participants from Cambridge, Somerville, Boston, Brookline, Chelsea, Everett, Winthrop, Revere and Quincy were seated in clusters representing the nine municipalities. Because influenza easily crosses jurisdictional boundaries, participants had to coordinate resources and communication. State health officials also participated in the drill, and worked to coordinate their response with local and state partners. To infuse the exercise with real urgency, training organizers incorporated a variety of technologies and communication devices. Participants staged conference calls and press conferences. The nine communities are members of the Boston Urban Area Security Initiative, a collaborative planning process funded by the Department of Homeland Security.
Source: http://www2.townonline.com/cambridge/localRegional/view.bg?a rticleid=345200

20. *October 13, Columbus Telegram (NE)* — **Nebraska conducts avian flu drill.** Health departments in Nebraska are preparing for a potential avian flu pandemic. The East Central District Health Department in Columbus, NE, will be creating a plan of action with selected law

enforcement officials and emergency management personnel on how to best handle the quarantine and isolation of infected people if the need should arise. Merrick County, NE, Emergency Management Agency officials are also preparing for a potential flu pandemic. The agency will hold a countywide public health emergency exercise Saturday, October 15. Agency officials say it's the first in the state, possibly the nation, to test countywide transportation as part of the plan. The exercise will utilize registration/pick−up sites around the county at seven locations where patients will park, be screened, register and be transported to a central dispensing site. They will then be processed, immunized, post−vaccine educated and returned to their buses for the trip back to where they started. Goals include the immunization of 250 patients each hour. Merrick County Emergency Management Agency, along with the Central District Health Department in cooperation with Merrick County's volunteer fire departments, Emergency Medical Services, Litzenberg Memorial County Hospital, law enforcement, schools and citizen volunteers will conduct the full−scale exercise.
Source: http://www.columbustelegram.com/articles/2005/10/12/news/new s4.txt

21. *October 13, Rocky Mountain News (CO)* — **Power failure disables freezers, cuts off security system at Centers for Disease Control and Prevention lab in Colorado.** A power failure knocked out the security system at a federal germ lab in Fort Collins, CO, for 13 hours Monday, October 10, and disabled freezers housing thousands of vials of plague and other potential bioweapons. A backup generator kicked on when the power failed. But an electrical short prevented the backup power from being routed through the building, said Colorado State University spokesperson Brad Bohlander. As a result, the Centers for Disease Control and Prevention (CDC) laboratory was without power for 13 hours, beginning at 3:07 p.m. MDT Monday. No germ collections were damaged, the public was not endangered, and no security breach occurred, said CDC spokesperson Jennifer Morcone. Extra security guards were posted during the blackout, which disabled the lab's video surveillance system and the electronic card keys that control access to restricted areas. Portable generators provided temporary power to the main germ freezers. Dry ice was used in smaller freezers, Bohlander said. The lab houses freeze−dried samples of about 1,000 plague strains, along with smaller collections of two other potential bioweapons, tularemia and Venezuelan equine encephalitis. West Nile virus and the microbes that cause Lyme disease and yellow fever also are stored at the lab.
Source: http://www.rockymountainnews.com/drmn/local/article/0,1299,D RMN_15_4154044,00.html

22. *October 12, National Journal's Technology Daily* — **Systems cannot combat flu pandemic, health officials say.** The American health care system does not have the information infrastructure needed to effectively combat a flu pandemic, leading health experts said Wednesday, October 12. The heart of the problem is not tracking influenza but getting critical information on outbreaks to doctors and local emergency responders and then back to crisis planners, Tara O'Toole, director of the Center for Biosecurity at the University of Pittsburgh, said at a Capitol Hill panel sponsored by Trust for America's Health. "Right now we have a very clunky system to allow the medical [community] to communicate," O'Toole said. Digital patient data would help alleviate the problem by letting doctors quickly transmit and share information about illness. The key to good communication about any spreading epidemic is accurate information, said Jeff Duchin, chief of communicable disease control at the University of Washington. "One of our challenges is to sort through the large amount of information coming across our screens to find out what is reliable," Duchin said. Internet bulletin boards

with backup systems on secure Websites would help, he added, but many local responders work outside cyberspace.
Source: http://govexec.com/story_page.cfm?articleid=32547&dcn=todays news

23. *October 11, U.S. Medicine* — **U.S. Government starts medical Website for Hurricane Katrina evacuees.** The federal government has teamed with local and state officials to establish a Website for authorized physicians to access the medication records and dosage information of Hurricane Katrina evacuees who they may be treating, in order to successfully transition care and avoid any prescription errors. The Website provides a secure service that allows physicians and pharmacists to renew critical medications, prescribe new ones, coordinate care, and avoid potential medication errors in the process. Launched Thursday, September 22, the Website contains information that was compiled and made available by medical software companies, chain pharmacies, local, state and federal agencies, a national foundation, electronic databases from commercial pharmacies, government health insurance programs such as Medicaid, private insurers, and pharmacy benefits managers in the states affected by the storm. The effort was facilitated by the Department of Health and Human Services Office of the National Coordinator for Health Information Technology and was supported by more than 150 organizations.
Medical Website: http://www.katrinahealth.org/
Source: http://www.usmedicine.com/dailyNews.cfm?dailyID=255

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

24. *October 13, Enid News (OK)* — **Terror test in Oklahoma designed to probe for weaknesses.** Enid, OK, will host a three−day, large−scale disaster drill next week in attempt to discover response weaknesses. Assistant Fire Chief Darrell Bundy said Enid and Garfield County emergency service agencies will be involved, along with Oklahoma Highway Patrol, Vance Air Force Base and the Army's 63rd Civil Support Team. The scenarios for the drills Monday, Tuesday and Wednesday, October 17−19, are based on terrorist events in Enid. Events Monday will be at the Enid water treatment plant. On Tuesday morning, the drill will be at the west gate of Vance Air Force Base. Tuesday afternoon, the drill will be at Mark Price Arena and Wednesday it will be at Clay Hall at Northern Oklahoma College in Enid. Both Enid hospitals will take part in the drill, along with Life Emergency Medical Services, Red Cross, and the Enid Area Radio Club. The disaster drill is good training for deputy fire chiefs and shift commanders and the city is working on the National Incident Management System, which theoretically has all entities using the same emergency plan. The drill is designed to increase communication between emergency entities.
Source: http://www.enidnews.com/localnews/local_story_286011204

25. *October 13, Providence Journal (RI)* — **Disaster drill aids Rhode Island town in revision of emergency operations plan.** Town officials in Coventry, RI, last week staged a Category 3 hurricane and the bombing of a chemical plant in a drill to test emergency response capabilities. The on−paper exercises, part of a two−day training session under the auspices of the state Emergency Management Agency, tested the officials' ability to make decisions quickly and aid the town's review of its emergency−operations plan, said Paul K. Sprague, Coventry's emergency management director. Although the emergency operations plan has long included an evacuation plan, that plan was revised and expanded following Hurricane Katrina, to give priority to evacuating Coventry's many mobile homes during a hurricane and moving residents to shelters, said Paul K. Sprague, Coventry's emergency management director. The town has more than 1,000 mobile homes, more than any other municipality in Rhode Island, he said. The participants grew noticeably better at communicating with one another by the second day, Sprague said. "The more you train, the more you communicate, the better off you are."
Source: http://www.projo.com/westbay/content/projo_20051013_cv13ema. 18401883.html

26. *October 13, San Francisco Examiner* — **Emergency drill helps California prepare for attack.** A five and a half hour disaster drill was conducted Wednesday, October 12, in San Francisco, CA, as a gauge of the city's preparedness for a disaster, whether natural or man−made. In the scenario, at 7:30 a.m. PDT a suicide bomber ripped apart a Muni bus. An hour later, another explosion occurred at the corner of Pine and Montgomery streets. The drill involved more than 200 city workers from departments such as police, fire, public health and public works, as well as state and federal officials. “We tried to stress the system, to see what San Francisco could handle and then we called in mutual aid. It was very successful,” said Annemarie Conroy, the head of the Office of Emergency Services and Homeland Security. Despite this, many emergency officials said the event also pointed out some deficiencies in San Francisco’s ability to respond to a disaster. They said the city needs easy access to a helicopter to observe a scene from the air, its emergency operations center is too small and it needs better coordination with surrounding jurisdictions to get ambulances to the scene of a disaster. Mayor Gavin Newsom said the city is working on each of the issues.
Source: http://www.sfexaminer.com/articles/2005/10/13/news/20051013_ne01_explosions.txt

27. *October 13, Los Angeles Times* — **Military's role to expand in disaster relief, disease outbreaks.** The Pentagon is planning to take a larger role responding to "catastrophic" events within the U.S. such as natural disasters and terrorist attacks and is developing plans to use active duty troops to respond to an avian flu pandemic, the Department of Defense's top homeland security official said Wednesday, October 12. The lessons from Hurricane Katrina require that the military assume a greater role during major disasters, said Assistant Secretary of Defense for Homeland Security Paul McHale. But McHale stressed that active duty troops would be used only for "catastrophic" events and would not be pulled into responding to the more than 50 storms, floods and hurricanes that require federal disaster assistance each year. McHale's remarks, during a breakfast meeting with defense writers on Wednesday, provided the first glimpse into the extent of the military's new mission. Government officials have yet to decide the scope of a disaster that would trigger a federal military response. With an annual budget of more than $400 billion and fleets of ships, helicopters and trucks at its disposal, the Pentagon is considered by many to be the only agency equipped to respond immediately to major national disasters.
Source: http://www.latimes.com/news/nationworld/nation/la−101205mili

tary_lat,0,7983083.story?coll=la-story-footer&track=morenews

[Return to top]

## Information Technology and Telecommunications Sector

28. *October 13, Security Focus* — **Symantec Brightmail AntiSpam malformed MIME message denial of service vulnerability.** Symantec Brightmail AntiSpam is susceptible to a denial of service vulnerability. This may cause a potential denial of service issue that has been identified and fixed in the Symantec Brightmail AntiSpam product.
Source: http://www.securityfocus.com/bid/15087/references

29. *October 12, Security Focus* — **Microsoft Windows FTP client directory traversal vulnerability.** Microsoft Windows FTP client is prone to a directory traversal vulnerability. This issue is due to a failure of the application to properly sanitize user supplied input. This vulnerability may cause a remote attacker to place files in an arbitrary location on a vulnerable computer. This can lead to data corruption or creation of potentially malicious files on a vulnerable computer.
Source: http://www.securityfocus.com/bid/12160/solution

30. *October 12, FrSIRT* — **VERITAS NetBackup bpjava-msvc remote format string vulnerability.** A vulnerability has been identified in VERITAS NetBackup servers and clients. This could be exploited by remote attackers to execute arbitrary commands. The vulnerability is due to a format string error in the Java authentication service "bpjava-msvc" that does not properly handle a specially crafted "COMMAND_LOGON_TO_MSERVER" command (port 13722), which could be exploited by remote attacker.
Source: http://www.frsirt.com/english/advisories/2005/2072

### 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 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** | 1026 (win−rpc), 5498 (hotline), 445 (microsoft−ds), 6346 (gnutella−svc), 135 (epmap), 6881 (bittorrent), 139 (netbios−ssn), 25 (smtp), 137 (netbios−ns), 1434 (ms−sql−m)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

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

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

## Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

## General Sector

Nothing to report.
[Return to top]

**DHS Daily Open Source Infrastructure Report Contact Information**

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

## DHS Daily Open Source Infrastructure Report Contact Information

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

## Contact DHS

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

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

## Department of Homeland Security Disclaimer