



# Department of Homeland Security Daily Open Source Infrastructure Report for 20 October 2005

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)  
<http://www.dhs.gov/>

## Daily Highlights

- The Associated Press reports Massachusetts Governor Mitt Romney has ordered emergency inspections for high-risk dams in the state, as a wooden dam in Taunton that was found in need of repairs in 2003 threatened to collapse and flood the city. (See item [9](#))
- The Agence France-Press reports Los Angeles International airport, a key U.S. hub for flights from Asia, is devising plans to quarantine hundreds of passengers suspected of carrying the deadly bird flu virus, should the need arise. (See item [16](#))

### DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

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

1. *October 19, Agence France-Press* — **OPEC expected to increase production capacity.** The Organization of the Petroleum Exporting Countries (OPEC) Secretary General Adnan Shihab-Eldin said at the annual meeting of the Asia-Pacific Economic Cooperation (APEC) forum on energy and mining in Gyeongju, South Korea, that OPEC will increase crude output by 5.5 million bpd (barrels per day) by 2009. He said: "Combined with a plan to increase production from OPEC from 32.5 million barrels a day to 38 million barrels a day by the year 2009 and an additional 1.5 million barrels a day of Natural Gas Liquids coming also from OPEC over the same period ... accumulative world oil production capacity (including

non-OPEC countries) will rise by around 12 million barrels a day over that period." He went on to say that this capacity will be above the demand for the period, which is estimated to be around seven to eight million barrels a day. Shihab-Eldin stated that the lack of refineries, rather than a lack of crude oil, is what is causing high oil prices. "It's very clear that currently, the market is well supplied with crude but the problem is that we don't have a refining system that can take all of the crude that is available," he said.

Source: <http://www.turkishpress.com/news.asp?id=75425>

2. *October 18, Associated Press* — **Greenspan projects energy prices to drag economy.** A rising demand for oil, spurred by increased use in Asian countries, has eliminated the slack in world oil markets that Federal Reserve Board Chairman Alan Greenspan said had kept oil prices relatively contained from 1985 through 2000. According to Greenspan, the oil market this year, however, "had been subject to a degree of strain not experienced in a generation." Since the oil shock of 1973, the amount of oil consumed per unit of economic output has fallen by one-third worldwide, and has been cut in half in the U.S. Greenspan says that these developments make the U.S. and global economies less susceptible to oil price shocks. He predicts that if high energy prices persist, countries will become even more energy-efficient.  
Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101800147.html>
  
3. *October 18, The Christian Science Monitor* — **Central Intelligence Agency invests in green energy.** The Central Intelligence Agency (CIA) through In-Q-Tel, a venture capital firm that they have set up to identify and invest in firms with cutting-edge technologies that can aid U.S. national security, has procured electricity-generating units fueled mostly by solar and wind energy. The units draw from a battery backup system in instances when the sun is down or the wind is calm. Designed to run for years with little maintenance, the units can generate up to 150 kilowatts of electricity, which is enough to power an emergency operations center, an Army field kitchen, or a small medical facility. The power stations could have important uses for disaster relief, homeland security, military operations, intelligence work, and a variety of commercial applications. The parts for the units are packed into standard-size shipping containers, which can be transported easily.  
Source: <http://www.csmonitor.com/2005/1018/p02s01-sten.html>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

4. *October 18, U.S. Immigration and Customs Enforcement Agency* — **Illegal workers arrested at defense contracting company.** Thirty-six foreign nationals who were illegally working in Durham, NC, for a government contractor were arrested on Tuesday, October 18. The arrests were part of the U.S. Immigration and Customs Enforcement (ICE) agency's strategy to

promote national security, protect critical infrastructure, and ensure fair labor standards in the workplace. The foreign nationals were working for a contractor that provides work to the Department of Defense, NASA, and the Department of Energy. Several workers had used invalid, altered, or falsified documents to illegally obtain employment. Those arrested were from Congo, the Gambia, Ghana, Guatemala, Indonesia, Israel, Kenya, Mexico, Pakistan, and Togo. In recent weeks, ICE agents have made other arrests at military facilities, including the arrest of three illegal aliens from Indonesia and Senegal on Wednesday, October 5, who served as language instructors at the U.S. Army Special Operations Command at Fort Bragg, NC. On Tuesday, October 4, seven illegal aliens were arrested at the U.S. Air Force Base in Mountain Home, ID. The men, from Canada and Mexico, were working for a construction company that was sub-contracted to build housing on the air base.

Source: [http://www.ice.gov/graphics/news/newsreleases/articles/05101\\_8durham.htm](http://www.ice.gov/graphics/news/newsreleases/articles/05101_8durham.htm)

[\[Return to top\]](#)

## **Banking and Finance Sector**

5. *October 19, Albuquerque Tribune (NM)* — **Summit attendees discuss identity theft.** Several law enforcement representatives in New Mexico, as well as national officials, attended a statewide summit to discuss identity theft Monday, October 17. The summit was put on by the New Mexico Securities Division Regulation and Licensing Department to discuss solutions to the growing problem. As it is, New Mexico is ranked twelfth in the number of identity-theft victims in the United States with 83.4 per 100,000 population in 2004, according to the Federal Trade Commission. Police Officer Matt Flotte said that identity theft is still not seen as a serious crime in the eyes of many law enforcement officers. "Most officers are still under the opinion that it's a secondary crime and don't realize the huge impact it has on its victims," he said.  
New Mexico Identity Theft Summit 2005: <http://www.rld.state.nm.us/Securities/index.htm>  
Source: [http://www.abqtrib.com/albq/nw\\_local/article/0,2564,ALBQ\\_198\\_58\\_4170111,00.html](http://www.abqtrib.com/albq/nw_local/article/0,2564,ALBQ_198_58_4170111,00.html)
6. *October 19, Mountain Home News (ID)* — **School district fears identity theft.** The Mountain Home School District in Idaho has notified its employees that its employee database may have been compromised and that they should be aware of potential identity theft problems. Superintendent Tim McMurtrey was notified by the Idaho State Police of the potential problem last week after Jerome County Sheriff's deputies arrested two people in a Twin Falls motel, originally on drug charges. In the course of their investigation authorities discovered a whole series of allegedly forged or stolen driver's licenses and \$17,000 in counterfeit checks. A number of the drivers licenses were in the names of Caldwell School District, ID, employees and several of the checks, which displayed the Caldwell School District logo on them, were apparently meant to be drawn on the Caldwell School District account. In addition, however, authorities also found a list of Mountain Home School District employees and their Social Security numbers. At present, there is not evidence to suggest those names or numbers had been used by the suspects, McMurtrey said. Mountain Home School District employs over 300 staff.  
Source: <http://www.mountainhomenews.com/story/1122701.html>
7. *October 18, Securities Industry Association* — **Business continuity test a success for financial services industry.** The Securities Industry Association (SIA), the Bond Market

Association, the Futures Industry Association and the Financial Information Forum on Saturday, October 15, conducted an industry-wide business continuity planning test as part of an extensive, ongoing and industry-driven initiative to verify and demonstrate the resilience of the securities markets. The test, which expanded on prior connectivity tests, included components for equities, fixed income, options, futures and settlement. "Backup data centers, work area recovery facilities and backup communications capabilities across the industry performed exceptionally well," said Don Kittell, executive vice president of SIA. During the test, firms and service bureaus accounting for more than 80 percent of the market's normal order volume connected simultaneously using backup data centers, backup communications links, alternate trading sites and alternate operations facilities to place test orders, executions and settlement interactions. There were no broad problems for any individual exchange or firm, and where issues arose, the vast majority were corrected when identified, allowing firms and exchanges to proceed with test orders. There were no problems that would have taken days to resolve or would have jeopardized operations in any major market segment, were they to occur in a real emergency.

Source: [http://www.sia.com/press/2005\\_press\\_releases/06889765.html](http://www.sia.com/press/2005_press_releases/06889765.html)

[[Return to top](#)]

## **Transportation and Border Security Sector**

- 8. *October 18, Department of Transportation* — FRA announces agreement with DM&E railroad.** Citing serious safety problems with track maintenance, employee training, bridge inspections, and highway-rail grade crossing warning systems, the Federal Railroad Administration (FRA) has signed an agreement with the Dakota, Minnesota & Eastern Railroad (DM&E) to bring the railroad into compliance with federal rail safety regulations. The safety compliance agreement with the Sioux Falls, SD-based railroad is the result of a series of inspections conducted by FRA in July and August that found numerous problems with the railroad's management and implementation of its safety program. The agreement requires the DM&E to develop and implement a detailed three-year track maintenance plan to address track defects, including fixing broken joint bars used to keep sections of track connected, and improving inspection practices. The railroad also must retrain managers on its operating rules and test employees in the areas where FRA found the most serious noncompliance, such as ensuring proper alignment of track switches and protecting the movement of rail cars from one train to another in rail yards. In addition, the railroad must adopt and implement an annual bridge inspection plan that provides for more frequent inspections based upon the condition of the bridge.

Source: <http://www.dot.gov/affairs/fra2605.htm>

- 9. *October 18, Associated Press* — Romney announces inspections of hazardous dams statewide.** Massachusetts Governor Mitt Romney on Tuesday, October 18, ordered emergency inspections for high-risk dams in the state, even as a wooden dam in Taunton that was found in need of repairs in 2003 threatened to collapse and flood the city. "We've had an unprecedented amount of rainfall in a short period of time, and the damage to these dams could be significant in some cases. We want to inspect them and make sure they're still in operable condition," Romney said. One of the Whittenton Pond Dam's new owners, Steve Poelaert, said Tuesday night that engineers and surveyors had been scheduled to begin work at the dam last week, but

put it off because of rain that led to high water now threatening the structure. Romney, along with state officials in charge of inspecting dams, painted a picture of a system that places too much responsibility for dam repair on the owners of private dams, like the threatened Whittenton Pond Dam in Taunton, and gives the state too few powers of enforcement. Bill Salomaa, the program manager of the Office of Dam Safety, said the state has been unable to keep up with oversight of the state's roughly 3,000 dams. Nine in ten of those are privately owned.

Source: [http://www.boston.com/news/local/massachusetts/articles/2005/10/18/romney\\_announces\\_inspections\\_of\\_hazardous\\_dams\\_stawew\\_ide/](http://www.boston.com/news/local/massachusetts/articles/2005/10/18/romney_announces_inspections_of_hazardous_dams_stawew_ide/)

- 10. *October 18, Department of Homeland Security* — Secretary Chertoff testifies on border security.** On Tuesday, October 18, Department of Homeland Security Secretary Michael Chertoff testified before the Senate Judiciary Committee on the vital issues of border security, interior enforcement and immigration reform. He said, "Ending illegal immigration means both tough enforcement and action to reduce the very demand that draws illegal migrants into the country. Therefore, our strategy of reforming our immigration system is a three-pillar, comprehensive approach that focuses on controlling the border, building a robust interior enforcement program, and establishing a Temporary Worker Program. A well-designed Temporary Worker Program will provide legal channels for U.S. employers and foreign born workers to match needs in the best interest of the U.S. economy without disadvantaging American workers."

Text of remarks: [http://www.dhs.gov/dhspublic/interapp/testimony/testimony\\_0040.xml](http://www.dhs.gov/dhspublic/interapp/testimony/testimony_0040.xml)

Source: <http://www.dhs.gov/dhspublic/>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report.

[\[Return to top\]](#)

## **Agriculture Sector**

- 11. *October 19, Reuters* — Hurricane menaces Florida citrus and sugar crops.** Hurricane Wilma may devastate prime citrus and sugar crops in Florida, officials warned on Wednesday, October 19. Florida's \$9.1 billion citrus industry is fretting about the storm and the cane plantations in the state also lie at risk. Florida's citrus industry was battered by three hurricanes that demolished 40 percent of last year's crop and spread the wind-borne bacteria that cause citrus canker disease. "Typically around this time of year we're already starting to harvest, but because of the hurricane impact last year and the stress on the trees, our crop is going to be later, about a month later, so Wilma would not be good news for us," said Casey Pace, spokesperson for Florida Citrus Mutual, the state's largest growers' association. The bigger fear is that another hurricane could spread canker-causing bacteria. Florida has fought for a decade to halt its spread. Regulators had hoped to eradicate the canker by the spring of 2007. Damage to Florida's sugarcane crop would come hard on the heels of Hurricane Rita lashing and flooding sugarcane fields in Louisiana, which is second to Florida for sugar in the U.S. Cane

industry officials in Louisiana said that up to 75 percent of production could be lost in areas where Rita's surge hit hardest.

Source: <http://today.reuters.com/business/newsarticle.aspx?type=BusinessNews&storyID=nN19293995>

12. *October 19, Southwest Farm Press* — **Retinal scans eyed for New Mexico show cattle.** New Mexico State University (NMSU) researchers are testing advanced eye-scanning technology on cattle as part of a national tracking system for animal health. “Retinal scans are part of a growing technological trend in cattle identification,” said Manny Encinias, livestock specialist at NMSU. “It flashes a beam of light into the eyeball and records the pattern of veins in the eye.” Each retina is unique and a scan is considered one of the most accurate forms of identification, he said. The NMSU evaluations are part of an accelerating effort by the U.S. Department of Agriculture to implement a National Animal Identification System. The goal is to track and identify all animals and premises that have had contact with an animal disease of concern within 48 hours of an initial diagnosis. Scientists tested 35 market steers from 18 Quay County farm families. Most of the cattle were show cattle. Encinias used a \$3,000 retinal scanner to record the IDs at three locations over a six-month period. The scanner makes an image, and downloads the data to a computer database. In addition to the retinal image, the device records the date, time, and a global positioning satellite coordinate of the location.
- Source: <http://southwestfarmpress.com/news/051119-retinal-show-cattle/>

13. *October 18, Associated Press* — **Plans to close farm offices scrapped.** The U.S. Department of Agriculture will abandon plans to close more than 700 local Farm Service Agency (FSA) offices across the country because of widespread opposition in Congress, an official said Tuesday, October 18. A hearing on the closures had been scheduled for Thursday, October 20, in the Senate Agriculture Committee. But in a letter sent Tuesday, October 18, to Chairman Saxby Chambliss, R-GA, Agriculture Department undersecretary J.B Penn said the agency is scrapping the plan. The plan was to close 713 of the 2,351 FSA offices, which are located in rural counties and connect farmers to government programs that provide payments and loans. The department said its aim was to modernize a system dating to the 1930s, but the plan faced resistance from lawmakers.
- Source: [http://www.businessweek.com/ap/financialnews/D8DAH16O8.htm?campaign\\_id=apn\\_home\\_down&chan=db](http://www.businessweek.com/ap/financialnews/D8DAH16O8.htm?campaign_id=apn_home_down&chan=db)

[\[Return to top\]](#)

## **Food Sector**

Nothing to report.

[\[Return to top\]](#)

## **Water Sector**

14. *October 18, Daily Herald (UT)* — **Chemical de-icer seeps into water supply.** Chemical de-icers have become the weapon of choice for improving traction on roads and highways across the Northwest. Their increase in use also has shown up in water samples taken from the

aquifer that underlies the Spokane Valley in Washington and parts of Northern Idaho. Experts in Idaho and Washington stress there's little cause for concern, but agencies in both states say they are keeping a close eye on the chemical's presence. In the 1980s, before the use of magnesium chloride, water samples from the aquifer would typically contain between one and two milligrams of chloride per liter. Since 1995, the average has risen to three to four milligrams. The drinking water standard for chloride set by the U.S. Environmental Protection Agency allows up to 250 milligrams per liter. But the growing presence of chloride is also an indication of the growing human impact to the aquifer. Chloride's fingerprint "may be a better indicator of other substances that are mobile in the environment that are also moving toward the aquifer, things we haven't thought yet of measuring," Dale Marcy, a chemistry and environmental science instructor at North Idaho College.

Source: <http://www.newutah.com/modules.php?op=modload&name=News&file=article&sid=66628>

[[Return to top](#)]

## **Public Health Sector**

**15. *October 19, Agence France–Presse* — New bird flu outbreaks reported.** Russia and China have confirmed new outbreaks of potentially lethal avian influenza. Russia's agriculture ministry said the H5N1 virus — already detected in Siberia in the summer — had been detected in the province of Tula, west of the Ural mountains, apparently borne by wild ducks. In Moscow, authorities confirmed that the virus in Tula was the H5N1 type. "We have confirmation from the laboratory that it is the H5N1 form" of bird flu, Nikolai Vlasov, deputy head of the ministry's veterinary control department, said. The announcement marks the first time the virus has arrived west of the Urals in Russia. Russia has culled hundreds of thousands of fowl and imposed numerous quarantines in a bid to wipe out the virus. In Beijing, authorities announced China's first reported outbreak of bird flu in more than two months, saying the disease had killed 2,600 birds, mostly chickens, on a farm in its northern Inner Mongolia region. The national bird flu laboratory confirmed that an epidemic on a farm near the Inner Mongolian capital of Hohhot was the H5N1 strain, the Xinhua news agency reported.  
Source: [http://news.yahoo.com/s/afp/20051019/hl\\_afp/healthfluworld\\_0\\_51019143804](http://news.yahoo.com/s/afp/20051019/hl_afp/healthfluworld_0_51019143804)

**16. *October 19, Agence France–Presse* — Los Angeles International airport works to prepare for avian flu quarantine of passengers.** Los Angeles, CA's airport, a key U.S. hub for flights from Asia, is scrambling to devise plans to quarantine hundreds of passengers suspected of carrying the deadly bird flu virus, officials said. As fears of a global pandemic of the flu that hit Asia two years ago grow, airport officials said they had been consulting with the US Centers for Disease Control and Prevention (CDC) for the last week to develop a plan to counter the spread of the deadly H5N1 Asian strain of disease if it arrived in the U.S. "We are trying to find the best facility that could house hundreds and hundreds of passengers," said Michael DiGirolamo, deputy executive director for Los Angeles World Airports. Los Angeles International is the United States' second busiest airport and one of the country's main gateways for travelers from Asia, with 26 daily flights arriving from across the Pacific carrying about 10,000 passengers.  
Source: [http://news.yahoo.com/s/afp/20051019/hl\\_afp/healthfluairport\\_losangeles\\_051019073514;\\_ylt=AjFcn9U4tzoyZFxSjhmkr8SJOrgF:ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCUI](http://news.yahoo.com/s/afp/20051019/hl_afp/healthfluairport_losangeles_051019073514;_ylt=AjFcn9U4tzoyZFxSjhmkr8SJOrgF:ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCUI)

17. *October 18, ABC News* — **Some doctors report shortage of flu shots.** Some doctors across the country have told ABC News they do not have enough flu shots for their patients and cannot get more from their suppliers. Medical professionals are particularly upset that supermarkets and department stores seem to have the vaccine. The current flu vaccine distribution system is enormously complicated, said William Schaffner, a professor of medicine in the division of infectious diseases at Vanderbilt University School of Medicine. The federal government orders very few adult vaccines and, as a consequence, has little control over distribution, he said. "Only half goes directly from the manufacturers to the end users (such as pharmacies). The other half goes through a very complex distribution chain, from one company to another to another, two or three times, before it gets to the end user," Schaffner said. The Food and Drug Administration said that occasional spot shortages may occur as manufacturers complete their final testing, but it expects them to be resolved as vaccine continues to be released to health care providers and others who administer the vaccine.  
Source: <http://abcnews.go.com/Health/Flu/story?id=1224517&page=1>

18. *October 18, University of Kentucky* — **Researchers to develop treatments for people exposed to dirty bomb.** Researchers from the University of Kentucky College of Pharmacy's Center for Pharmaceutical Science and Technology (CPST), in partnership with a pharmaceutical company, have received \$1.2 million in funding from the National Institutes of Health (NIH) to develop treatments to be used in radiation emergencies such as after exposure to dirty bombs. In May, the NIH's National Institute of Allergy and Infectious Diseases (NIAID) solicited proposals to develop alternative formulations or delivery methods that help clear the body of radioactive elements to be used in a mass exposure situation. According to the NIAID, the potential for radiation exposures to occur from terrorists acts, radiation accidents or nuclear detonation mandates that the health care system develop and implement preparedness plans that include the stockpiling of radioprotective drugs and therapeutics. Currently, radioactive materials must be removed from the body by administering intravenous drugs. However, the researchers are proposing to develop an orally administered dosage formulation with the ultimate goal of identifying an effective treatment for inclusion in the Strategic National Stockpile. NIAID is facilitating the development of this project because oral formulations would be easier to distribute and administer during a mass exposure situation.  
Source: [http://news.uky.edu/news/display\\_article.php?category=1&articleid=681](http://news.uky.edu/news/display_article.php?category=1&articleid=681)

[\[Return to top\]](#)

## **Government Sector**

19. *October 14, Government Accountability Office* — **GAO-06-106: State Department: Stronger Action Needed to Improve Oversight and Assess Risks of the Summer Work Travel and Trainee Categories of the Exchange Visitor Program (Report).** Past Government Accountability Office (GAO) and the Department of State (State) Office of Inspector General reviews have reported that some exchange visitors have participated in unauthorized activities and cited problems in the management and oversight of the programs. Strong management oversight is needed to ensure that the programs operate as intended and are not abused. This report examines how State manages the Summer Work Travel and the Trainee programs to ensure that only authorized activities are carried out under the programs and



identifies potential risks of the programs and the data available to assess these risks. A number of potential risks are associated with the programs, including that exchange visitors might use it to remain in the United States beyond their authorized time. This report recommends that the Secretary of State take strong action to enhance the overall management and monitoring of the Summer Work Travel and Trainee programs, including fully implementing a compliance unit to monitor exchange activities; updating and amending regulations; and developing strategies to obtain data on overstays, program abuses, and other risks associated with the programs. State acknowledged weaknesses in the programs and described actions it is taking to address our recommendations.

Highlights: <http://www.gao.gov/highlights/d06106high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-106>

[\[Return to top\]](#)

## **Emergency Services Sector**

**20. *October 19, Statesman Journal (OR)* — Legislature will appoint panel to study Oregon's disaster readiness.** Oregon's legislative leaders are creating an emergency-preparedness committee to review government plans for dealing with potentially catastrophic events, such as a flu pandemic, an earthquake or a tsunami. Oregon Senate President Peter Courtney said he and House Speaker Karen Minnis have agreed to appoint a joint interim panel to look at the state of disaster readiness in government. Courtney said the leaders need to keep the public focused on what's being done to prepare. The state's top health official, meanwhile, said she thinks Oregon's public-health system is prepared to respond to a flu pandemic. Dr. Susan Allan, the public-health director in the state Human Services Department, said the state has a general disease-management plan and a specific flu-pandemic plan based on "trying to contain any outbreak while it's still small." Every local health department has a full-time emergency planner, she said. Systems are set up for doctors to contact state authorities and for the state to contact the federal Centers for Disease Control and Prevention at the first occurrence of a serious disease. A statewide drill is set for Wednesday, November 2, to deliver medicine and supplies to communities from what is known as the "strategic national stockpile."  
Source: [http://159.54.226.83/apps/pbcs.dll/article?AID=/20051019/STA\\_TE/510190325/1042](http://159.54.226.83/apps/pbcs.dll/article?AID=/20051019/STA_TE/510190325/1042)

**21. *October 18, Government Technology* — Virginia sponsors five-state drill to test emergency preparedness and response.** With Hurricane Katrina reminding the entire country of the importance of emergency preparedness, the Virginia Department of Health (VDH) is sponsoring a five-state exercise to test emergency planning efforts. Virginia will partner with Kentucky, North Carolina, Tennessee and West Virginia to test and evaluate response efforts during a mock exercise on Monday, October 24, through Thursday, October 27, in the western areas of the state. VDH's Emergency Preparedness and Response Programs and the Virginia Department of Emergency Management routinely coordinate and conduct exercises to evaluate emergency response plans and procedures. This year's event, called OctoberTEST, will not only test localities, agencies and hospitals on how well they work together to respond to a series of fictional emergency public health events, but it will also assess the ability to work across state lines. This year's drill will focus on a series of simulated disease outbreaks which will escalate into a full-scale, multi-state response to a suspected act of bioterrorism. Participants will combine table-top sessions with actual demonstrations such as mock victims entering hospitals

and health department offices to report symptoms, mock media arriving to cover the developments, and the staging of mass dispensing sites to deliver medicines to the exposed populations.

Source: [http://www.govtech.net/magazine/channel\\_story.php/96990](http://www.govtech.net/magazine/channel_story.php/96990)

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

### **22. *October 19, Washington Post* — Sleuths crack tracking code discovered in color printers.**

An invisible bar code of sorts that contains the serial number of the printer as well as the date and time a document was printed has been cracked by the Electronic Frontier Foundation (EFF), a San Francisco consumer privacy group. According to U.S. Secret Service spokesperson Eric Zahren, "It's strictly a countermeasure to prevent illegal activity specific to counterfeiting. It's to protect our currency and to protect people's hard-earned money. "

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html?referrer=email>

### **23. *October 18, CNET News* — Schools get tailored cyberattack data.** U.S. colleges and universities are getting a service that analyzes security data to help fend off cyberattacks. According to Steffani Burd, the executive director of Information Security in Academic Institutions, "The goal is to have an accurate assessment of information security in academic institutions." The project is sponsored by the research arm of the U.S. Department of Justice and run by Columbia University's Teachers College in New York. Academic organizations will be expected to submit logs from their firewall and intrusion detection systems so the service can parse the data and generate reports on attacks. Those reports can then be used to protect networks. Johannes Ullrich, the chief research officer at the SANS Institute and founder of DShield.org states, "Academic institutions face the challenge of maintaining an open network while also providing security for their users. This data will help them decide what protection to deploy while minimizing restrictions."

Source: [http://news.com.com/Schools+get+tailored+cyberattack+data/2100-7347\\_3-5900684.html?tag=cd.top](http://news.com.com/Schools+get+tailored+cyberattack+data/2100-7347_3-5900684.html?tag=cd.top)

### **24. *October 18, Security Focus* — Oracle October security update multiple vulnerabilities.**

Various Oracle Database Server, Oracle Enterprise Manager, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and Applications, and Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne are affected by multiple vulnerabilities. The issues identified by the vendor affect security properties of the Oracle products and present local and remote threats. Oracle has released a Critical Patch Update advisory for October 2005 to address these vulnerabilities. This Critical Patch Update addresses the vulnerabilities for supported releases.

Oracle Critical Patch update: <http://www.oracle.com/technology/depoy/security/pdf/cpuoct2005.html>

Source: <http://www.securityfocus.com/bid/15134/info>

## DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

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

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

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

Top Source Port / IP Addresses: Increased reported port activity: 1026 UDP, 1026 UDP, 1029 UDP, 1030 UPD from the following IP blocks, located in China:  
221.10.254.31,218. 66.104.208, 222.77.185.242, 221.27.16.180, 61.152.158.126, 221.6.77.72, 202.99.172.160, and 218.66.104.206

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

### Current Port Attacks

<b>Top 10 Target Ports</b>	6346 (gnutella-svc), 1026 (win-rpc), 6881 (bittorrent), 445 (microsoft-ds), 26777 (----), 135 (epmap), 139 (netbios-ssn), 40000 (----), 25 (smtp), 1025 (win-rpc) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://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 <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> 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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.