Department of Homeland Security Daily Open Source Infrastructure Report for 25 October 2006

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

Daily Highlights

- ABC−7 reports an apparent security flaw in the computers that contain personal information on hundreds of thousands of voters in Chicago enabled a non−partisan organization to gain access to sensitive personal information including Social Security numbers. (See item 11)
- The Associated Press reports Tennessee's Emergency Communications Board has voted to begin a statewide project to modernize the infrastructure by linking all of its call centers with a digital network, Next Generation 911. (See item 32)

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 24, Associated Press* — **Power line is planned for Southwest.** Montana Governor Brian Schweitzer and industry executives announced plans Monday, October 23, to build a $2−billion power transmission line that would carry energy to the fast−growing cities of the Southwest. If the line is successfully completed, it would run from the coal fields of Montana to Las Vegas, Los Angeles, and Phoenix. It would carry electricity created by either wind power or synthetic gas derived from coal to meet clean energy requirements in the Southwest and serve 3.5 million people. Developers hope to complete the project by 2011, said Brad Thompson of TransCanada. The transmission line would travel west from eastern Montana and

turn south through Idaho on its way to Nevada. Connectors from the Las Vegas area would run to Los Angeles and Phoenix.
Source: http://www.latimes.com/business/la−fi−power24oct24,1,7864267.story?coll=la−headlines−business

2. *October 24, Associated Press* — **Accident kills one in Pennsylvania coal mine.** Dale Reightler was killed Monday, October 23, in an explosion at a Schuylkill County, PA, coal mine. Five other miners escaped. The accident happened about a half mile underground at an R&D Coal Co. anthracite mine in a remote region of Tremont Township, about 80 miles northwest of Philadelphia. It appeared the blast occurred when miners detonated explosives, said Dirk Fillpot, spokesperson for the federal Mine Safety and Health Administration. The miners had checked for methane gas before the 10:30 a.m. EDT detonation but didn't detect any, he said. Less than two years ago, four workers at the same mine were injured by flying debris and coal from an explosion caused by a pipe with a faulty gauge, according to state officials. R&D was allowed to reopen after installing safety equipment following the accident.
Source: http://www.chron.com/disp/story.mpl/nation/4282733.html

3. *October 24, Washington Post* — **Shell seeks to buy Canadian oil sands unit, tap supply source for U.S.** Royal Dutch Shell PLC has offered to pay $6.8 billion for the outstanding shares of Shell Canada Ltd. and gain a greater stake in Canada's oil sands. Shell Canada, which is 78 percent owned by Royal Dutch Shell, operates an oil−sands project in the Athabasca region of northeastern Alberta province. John Hofmeister of Shell Oil Co., the U.S. subsidiary of Royal Dutch/Shell Group, said that the oil sands would be a "great boost" to the company and a "great supply source for the United States." The reserves of Canada's oil sands are second in size only to Saudi Arabia's reserves. Total production from Canada's oil sands is about one million barrels a day and oil companies expect that volume to triple or quadruple over time. Hofmeister also said that the company would be better able to plan across the U.S.−Canada border. That could become more important in the future, when the company may need to ship oil to U.S. refineries capable of turning the heavy oil sands crude into petroleum products such as gasoline or heating oil.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/23/AR2006102300241.html

4. *October 21, Philadelphia Inquirer* — **Thousands lose electricity as winds topple power lines.** Strong winds knocked down trees and power lines throughout the region Friday, October 20, leaving thousands of northeast residents without power. Peco Energy Co. reported that as many as 75,000 customers lost power, but that service was restored to all but 15,000 later that evening. Public Service Enterprise Group reported about 2,200 outages in New Jersey.
Source: http://www.philly.com/mld/inquirer/news/local/states/new_jersey/15813910.htm?source=rss&channel=inquirer_new_jersey

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *October 23, WCPO (OH)* — **Ammonia leak prompts shelter−in−place in Ohio.** An ammonia

leak made at least eight workers sick at a West Chester, OH, factory late Sunday night, October 22. Just after midnight, some workers at the U.S. Food Service plant started to notice their lungs burning and breathing becoming difficult. A leak of up to 1,000 pounds of anhydrous ammonia leaked from a broken coil in a refrigeration system, causing the factory to be evacuated. Eight people working inside the food processing plant were either treated at the scene or taken to hospitals for further evaluation. A shelter−in−place order was set up for people living or working within one square mile of the plant.
Source: http://www.wcpo.com/news/2006/local/10/23/ammonia_leak.html

[Return to top]

Defense Industrial Base Sector

6. *October 24, Defense Industry Daily* — **UK unveils Defense Technology Strategy.** Britain has made significant strides in changing its overall approach to defense acquisition over the past few years, from the proliferation of long−term support partnerships and a move toward true through−life equipment management for key military platforms to the SMART Acquisition initiative and the UK Defense Industrial Strategy released in December 2005. As part of those broader efforts, the UK Ministry of Defense (MOD) recently released their Defense Technology Strategy, which sets longer−term research and development (R&D) priorities. With an annual spend of approximately $4.9 billion, the MOD is a very large investor in R&D. This new strategy sets out in detail those technologies which the MOD believes should be supported and brought from concept to front line delivery more quickly.
Full text report: http://www.mod.uk/NR/rdonlyres/27787990−42BD−4883−95C0−B48BB72BC982/0/dts_complete.pdf
Source: http://www.defenseindustrydaily.com/2006/10/uk−unveils−defence−technology−strategy/index.php

7. *September 21, Government Accountability Office* — **GAO−06−1042: Influenza Pandemic: DoD Has Taken Important Actions to Prepare, but Accountability, Funding, and Communications Need to be Clearer and Focused Departmentwide (Report).** An influenza pandemic would be of global and national significance and could affect large numbers of Department of Defense (DoD) personnel, seriously challenging DoD's readiness. The Government Accountability Office (GAO) was asked to examine DoD's pandemic influenza preparedness efforts. This report focuses on DoD's planning for its workforce, specifically (1) actions DoD has taken to prepare and (2) challenges DoD faces going forward. GAO analyzed guidance, contracts, and plans, and met with DoD officials. GAO recommends that DoD: (1) define and communicate roles and responsibilities, oversight mechanisms, and goals and performance measures for DoD's efforts, (2) establish a framework to request funding, tied to its goals, (3) define and communicate departmentwide which types of personnel DoD plans to include in its vaccine and antiviral distribution, and (4) implement a comprehensive and effective departmentwide communications strategy. DoD generally concurred with four recommendations, and did not address one in its written comments. Based on DoD's comments and additional information provided showing DoD designated a lead authority for its efforts, GAO combined two recommendations. GAO clarified another recommendation to focus on requesting funding tied to the department's goals.
Highlights: http://www.gao.gov/highlights/d061042high.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−1042

[Return to top]

Banking and Finance Sector

8. *October 24, Washington Post* — **Hackers zero in on online stock accounts.** Hackers have been breaking into customer accounts at large online brokerages in the U.S. and making unauthorized trades worth millions of dollars as part of a fast−growing new form of online fraud under investigation by federal authorities. E−Trade Financial Corp. said last week that "concerted rings" in Eastern Europe and Thailand caused their customers $18 million in losses in the third quarter alone. TD Ameritrade also has suffered losses from customer account fraud. "It is an industry problem," spokesperson Katrina Becker said. Federal regulators say that the fraud is fed by the rising use of the Internet for personal finance and the easy availability of snooping software that allows hackers to steal personal account information. More than 10 million people have bought or sold investments online in the United States in the last few months, according to Gartner Inc. The scams typically begin with a hacker obtaining customer passwords and user names. One way is by placing keystroke−monitoring software on any public computer. Hackers wait until anyone types in the Web address of an online broker, and then watch the next several dozen keystrokes, which are likely to include someone's password and login name.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/23/AR2006102301257_pf.html

9. *October 24, Register (UK)* — **Hacking contactless credit cards made easy.** U.S. security researchers have demonstrated how easy it might be for crooks to read sensitive personal information from RFID−based credit and debit cards. Researchers from the RFID Consortium for Security and Privacy have shown how crooks might be able to skim sensitive information from cards −− including card number, expiration, and issue dates, and a cardholder's name −− without actually physically stealing the latest generation of credit cards. The attack uses off−the−shelf radio and card reader equipment that could cost as little as $150. Although the attack fails to yield verification codes normally needed to make online purchases, it would still be possible for crooks to use the data to order goods and services from online stores that don't request this information. Despite assurances by the issuing companies that data contained on RFID−based credit cards would be encrypted, the researchers found that the majority of cards they tested did not use encryption or other data protection technology.
Source: http://www.channelregister.co.uk/2006/10/24/rfid_credit_card_hack/

10. *October 23, St. Louis Post−Dispatch* — **Woman sentenced in bank check scam using information from political flyer.** A Metro East, MO, woman who used bank information gleaned from copies of checks on an accusatory political flyer to scam the Village of Washington Park into paying $170,000 of personal expenses for herself and others was sentenced to 33 months in federal prison. In late 2002, Takisha Walker found a flyer on her door that accused a politician of misusing Village of Washington Park funds for personal expenses. She took the bank and routing numbers from the copies of the checks on the flyer, and paid her own personal expenses, court documents show. From October 2002 through December 2003, Walker used an online bill−paying service to pay cell phone and utility bills,

car payments, mortgages, and other bills for herself and others, according to court documents and then−Mayor Sherman Sorrell in 2004. Those people would then kick money back to Walker.
Source: http://www.stltoday.com/stltoday/news/stories.nsf/metroeast/story/9ED6251469175DF4862572100068B523?

11. *October 23, ABC−7 (IL)* — **Apparent security flaw in board of elections Website.** An apparent security flaw in the computers that contain personal information on hundreds of thousands of voters in Chicago enabled a non−partisan organization to gain access to sensitive personal information including Social Security numbers. The group claims someone with evil intentions could do the same thing and disrupt the entire election. The problem has only to do with the board of elections Website, not the voting machines themselves. Nevertheless, the Illinois Ballot Integrity Project say that someone conceivably could have confused voters by logging into the system and making changes. The board of elections says they have no reason to believe any of that has happened thus far. The Chicago Board of Elections Website gets hundreds of thousands of visitors during election season. According to the Illinois Ballot Integrity Project, they could also get personal information about nearly 800,000 voters, including date of birth and Social Security numbers. The board of elections had closed access to this information but it was still on their database, and were unaware that users could view the information. The board says it is taking steps to ensure no one has used the information for identity theft purposes.
Source: http://abclocal.go.com/wls/story?section=local&id=4688529

[Return to top]

Transportation and Border Security Sector

12. *October 24, Times−Herald Record (NY)* — **Threat closes Port Authority Bus Terminal.** A 28−year−old Pennsylvania man, described as "emotionally distressed," was in police custody Monday night, October 23, after provoking an incident that closed the Port Authority Bus Terminal in New York, for more than two hours, officials say. The man, who was not otherwise identified, clung to his bag and refused to get off a Trailways bus that arrived at the terminal around 1 p.m. EDT, according to Marc La Vorgna, a Port Authority spokesperson. When Port Authority and New York City police were unable to coax him off the bus, the agency told bus companies around 2 p.m. to suspend operations and shuttered the south wing of the terminal. NJ Transit and Short Line subsequently put employees on the street in an attempt to corral the first customers of the evening rush and direct them to waiting buses on 9th and 10th Avenues. The closing, albeit only two hours, affected hundreds of buses and thousands of customers. The confusion and delays stretched into the evening. A New York City police negotiator ultimately talked the man off the bus. A bomb squad examined the bag, swept the bus, and found nothing.
Source: http://www.recordonline.com/apps/pbcs.dll/article?AID=/20061024/NEWS/610240313

13. *October 24, Washington Post* — **Rocks hurled onto Capital Beltway damage at least 21 vehicles.** The hail of rocks and bricks that rained down on the Capital Beltway this past weekend pelted at least 21 vehicles, breaking windshields and denting hoods, and more drivers called in Monday, October 23, to report damage to vehicles, according to the Maryland State

Police. Police said the nature of the crime has led them to suspect that juveniles were responsible for throwing the debris off the Temple Hill Road overpass Saturday night, October 21, onto the inner loop of Interstate 495 in Temple Hills. Although such incidents occasionally happen on the Beltway and elsewhere, the scope of the damage struck some police officers as far beyond normal. "This is the most I've ever seen. . . . Normally, it's one or two or three. This is a bit much," said Maryland State Trooper 1st Class Gary Matthias. "We were fortunate that there were not any injuries." In addition to the state police, the Prince George's County police and a U.S. Park Police helicopter helped search for suspects, but none were found. Matthias thinks more than one person was responsible, and police are investigating whether the debris was taken from the Woodrow Wilson Bridge construction site nearby.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/23/AR2006102301115.html

14. *October 23, RFID Journal* — **RFID adds to security at Virginia Port Authority.** The Virginia Port Authority is deploying radio frequency identification (RFID) systems to improve the security and efficiency of the processes surrounding its cargo container shipments. The authority is joining a growing number of ports worldwide that are deploying RFID technologies for tracking security. Sensors are optional, but if used, the RFID tags can record whether a container door has been opened or closed, or whether there has been any shock to the container. These sensors can also detect changes in humidity or temperature measurements. The Port of Virginia has three separate terminals: Norfolk International Terminal, Newport News Marine Terminal and Portsmouth Marine Terminal. Within the next month, the Virginia port will have RFID readers and antennas operating at all three terminals, says Ed Merkle, director of port security and emergency operations for the Virginia Port Authority.
Source: http://www.rfidjournal.com/article/articleview/2748/1/1/

15. *October 18, 24dash.com (United Kingdom)* — **'Major security flaws' in the air cargo industry revealed.** Cargo on passenger flights is being sent without checks or X−rays in oversights that could potentially threaten the lives of passengers, BBC Radio 4's The World Tonight said on Tuesday, October 17. The security gaps emerged following a drug smuggling case at Kingston Crown Court in southwest London. The BBC said it began an investigation when the hearing revealed that the "known shipper" system used by air courier and cargo companies had been broken by drug smugglers and used to import large amounts of cocaine into the UK from America. During the case, a former employee of Federal Express (FedEx) admitted selling the confidential account numbers of reputable firms at FedEx's depot in Vauxhall, south London, the BBC said. This reportedly allowed a student and his accomplices abroad to smuggle in drugs using the security clearance and accounts of innocent companies. The BBC also reported that Brian Fenn, head of UK security for FedEx, admitted in evidence during the case that the known shipper system could also potentially be used to smuggle a bomb on to a plane undetected. The BBC said its investigation revealed that the Web−based system for tracking parcels could be used by terrorists to target particular flights.
Source: http://www.24dash.com/communities/11750.htm

16. *September 22, Government Accountability Office* — **GAO−06−979: Coast Guard: Condition of Some Aids−to−Navigation and Domestic Icebreaking Vessels Has Declined; Effect on Mission Performance Appears Mixed (Report).** The marine transportation system is a critical part of the nation’s infrastructure. To facilitate the safety and efficiency of this system, the

Coast Guard maintains aids−to−navigation (ATON), such as buoys and beacons, and conducts domestic icebreaking in the Great Lakes, St. Lawrence Seaway, and northeast coast. To conduct these missions, the Coast Guard has a fleet of more than 200 vessels, ranging from 225−foot seagoing buoy tenders and 140−foot domestic icebreakers to 21−foot boats. After the terrorist attacks of September 11, 2001, many of these assets took on additional responsibilities for security patrols and other homeland security duties. Although some assets have been recently acquired, many others are reaching or have exceeded their design service lives, raising concerns about how well and for how much longer these older assets may be able to carry out their missions. The Government Accountability Office (GAO) examined (1) recent trends in the amount of time these assets have spent performing missions; (2) asset condition and its effect on mission performance; and (3) the actions taken by the Coast Guard to continue to achieve the missions of these assets. To conduct this work, GAO reviewed Coast Guard documents, interviewed Coast Guard officials, and made site visits to various locations.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−979

[Return to top]

Postal and Shipping Sector

17. *October 23, Daily Bulletin (CA)* — **Indictment reveals postal workers in identity thefts.** Postal workers from the Industry Processing and Distribution Center stole refund checks and credit cards from the mail that they sold to an identity theft ring. Using bogus IDs, members of the ring cashed the checks and used the cards to get cash advances or buy merchandise. The losses totaled $1 million in three and a half years. Federal officials announced details, along with other cases investigated by a new identity theft task force in Orange County, CA. The investigation on the ring was dubbed "Operation Paper or Plastic." The postal workers met with members of the ring at coffee shops and other spots in Orange County. From January 2003 to August 2006, the ring cashed checks at banks in Los Angeles, Nevada, Arizona, Georgia, New Mexico, and Missouri, and used credit cards in casinos and banks in several cities. The indictment doesn't say how many employees were involved or when the mail was stolen. The workers were only stealing treasury checks and credit cards. The checks and cards stolen were supposed to be mailed to people living in ZIP codes beginning in 917, 918, 926, 927, and 928. The U.S. Postal Inspection Service is investigating the mail thefts.
Source: http://www.dailybulletin.com/news/ci_4533501

18. *October 23, Reuters* — **Stop mailing fake grenades, Canadians told.** Tired of having its offices evacuated due to false alarms, Canada's postal system officials said on Monday, October 23, that it will no longer transport replica and inert military explosives. Canada Post said that fake and inoperative grenades and artillery shells have caused "numerous" evacuations of post offices in recent years, which have disrupted the flow of mail and scared employees. "Continued exposure to these replica or inert munitions poses a real danger and desensitizes Canada Post and Canada Border Services Agency employees to instances where there may be a genuine explosive device," it said in a statement. Canada Post already prohibits the mailing of live grenades and other explosives, according to its Website.
Source: http://ca.today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006−10−23T215356Z_01_N23404424_RTRIDST_0_CANADA−LIFE−CANADA−MAIL−COL.XML

19. *October 23, DM News* — **UPS, Poste Italiane strike deal on express international shipments.** United Parcel Service (UPS) and Poste Italiane have completed an agreement for UPS to carry the Italian postal service's international express shipments. The service is scheduled to start November 27 for the 14,000 post offices Poste Italiane operates across Italy. UPS, Atlanta, also said it is finalizing details to use the Poste Italiane network for its own pickup and final delivery in certain extended areas of Italy. The UPS venture with Rome−based Poste Italiane is part of its strategy to make it easier for shippers everywhere to access global markets. The partnership with UPS is also part of Poste Italiane's strategy to strengthen its position in the express courier domestic market. In addition to its core postal services, the Poste Italiane Group offers communication, logistic and financial services across Italy.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/38678.html

[Return to top]

Agriculture Sector

20. *October 24, Southeast Farm Press* — **Stripe rust spreading in Southeast wheat.** Asian soybean rust isn't the only rust to threaten U.S. crop fields. Wheat farmers face their own corrosive crop disease called stripe rust. It has devastated high yielding, yet susceptible wheat varieties in recent years. According to the U.S. Department of Agriculture's Agricultural Research Service, yield losses of 40 percent are common, and some fields are completely destroyed. During the 2005−06 growing season, overall disease pressure on wheat was light with the exception of stripe rust, reports Georgia Extension agronomist Dewey Lee. University of Georgia Small Grains Breeder Jerry Johnson says stripe rust is a relatively new problem for growers in the Southeast. "Historically, stripe rust has been a problem in the Pacific Northwest and California," he says. "Eight to 10 years ago, it moved to Louisiana, east Tennessee and Arkansas. Then, two to three years ago, it moved here. This disease is just getting to the East Coast. There has been less stripe rust in the Carolinas than in Georgia and Arkansas."
Source: http://southeastfarmpress.com/news/102406−stripe−rust/

21. *October 23, World Organization for Animal Health* — **Bluetongue in Northern Europe: OIE Reference Laboratory makes a breakthrough in identifying the vector causing the disease.** The OIE Reference Laboratory in Teramo, Italy, established that an insect adapted to the European climate acted as the vector responsible for the recent bluetongue outbreaks in Northern Europe. The vector, a biting midge of the culicoides species was identified as Culicoides dewulfi. "It is an important new epidemiological event because previously all bluetongue outbreaks were linked to an African vector. This suggests the disease could now stay in all the region with the risk of more cases occurring in spring when the vector activity is very high", Dr. Bernard Vallat, Director General of the World Organization for Animal Health said. Bluetongue is an insect−borne viral disease to which all species of ruminants are susceptible. The disease poses no danger to human health. It occurs mostly during periods of high temperature and rainfall and usually disappears with the first frost or severe cold weather, when midges stop their activity.
Source: http://www.oie.int/fr/press/fr_061023.htm

22.

October 22, Daily Sentinel (CO) — **Combination of beetle, fungi may eradicate noxious weed.** The marriage of a fungus and a tiny beetle might be the key to wiping out uncontrolled growth of leafy spurge, new research from Mesa State College in Grand Junction, CO, and the Colorado Department of Agriculture suggests. A small team of researchers led by Mesa State plant pathologist Margot Becktell is using a combination of beetles and soil−borne fungi to naturally control growth of the highly invasive weed that has displaced native plants and made many Colorado grazing pastures worthless. The demise of a leafy spurge begins when adult flea beetles eat away at the plant's leaves. Soon, the beetles lay eggs that fall around the base of the plant. Once the eggs hatch, the larvae burrow underground to feed on the roots, essentially "choking" the plant, Becktell said. More importantly, the larvae chew holes into the roots, making them more susceptible to the fungi in the soil.
Source: http://www.gjsentinel.com/news/content/news/stories/2006/10/22/10_23_1a_leafy_spurge.html

[Return to top]

Food Sector

23. *October 24, Agricultural Research Service* — **Unraveling the Listeria genome.** Scientists at the Agricultural Research Service Eastern Regional Research Center in Wyndmoor, PA, and the Institute for Genomic Research in Rockville, MD, have sequenced the genomes of four Listeria monocytogenes strains, representing three serotypes. The research team found that Listeria strains, in addition to sharing serotype−specific and strain−specific genome sequences, have largely similar genetic content and organization. The scientists also confirmed that Listeria strains have 15 genes in the Crp/Fnr regulatory protein family, which is considerably more than most bacteria. The team is investigating whether these sequences influence the bacterium's virulence or persistence. Knowing more about L. monocytogenes will help regulatory agencies and members of the food industry make informed decisions about control strategies and safety standards. In addition, uncovering the genetic information that defines Listeria's characteristics and behavior will help scientists understand the bacterium's virulence and persistence. This research will be useful in preventing Listeria contamination and in reducing disease. It could also aid decisions about managing the threat of foodborne listeriosis.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

24. *October 23, Food Safety and Inspection Service* — **Connecticut firm recalls ground beef products for possible E. coli O157:H7 contamination.** Omaha Beef Company, Inc. is voluntarily recalling approximately 1,680 pounds of ground beef products that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) announced Monday, October 23. The products subject to recall include 10−pound boxes of hamburger patties and five− and 10−pound bags of hamburger. Each package bears the establishment number "Est. 2769" inside the USDA mark of inspection, as well as the case code, "101861." The problem was discovered through routine FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of these products. The ground beef products were produced on October 18 and were distributed to restaurants in Connecticut and several counties in southern New York State. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration. The very young, seniors and persons with compromised immune systems are the most susceptible to

foodborne illness.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_031_2006_Relea se/index.asp

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

25. *October 24, Agence France−Presse* — **Polio spreads in India.** India has reported 416 cases of polio this year −− more than a quarter of the world total, a senior federal health ministry official has said. "From Uttar Pradesh, the disease is spreading to states where there were no endemic transmissions −− including Punjab and Haryana and Maharashtra," the official said. The spike in the number of cases, after just 66 were reported in 2005, has prompted New Delhi to launch an emergency immunization drive to vaccinate 120 million children in the second week of November, he said. "From three percent of the global cases in 2005, we now have 26 percent of global cases," he added.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://news.yahoo.com/s/afp/20061024/hl_afp/indiahealthpolio_061024102431

26. *October 24, RIA Novosti (Russia)* — **Russia tests bird flu vaccine.** Clinical tests of a bird flu vaccine, developed by the Russian Health Ministry's state−owned Science and Production Association Mikrogen in conjunction with the Academy of Medical Sciences, have been conducted in the last three months. The tests involved 240 healthy volunteers, separated into two groups numbering 120 men and women each. Vitaly Zverev, director of the Mechnikov Vaccine and Serum Research Institute, said a study of post−vaccination side effects showed the preparation was well tolerated, safe, and did not produce any serious negative effects. Vaccine developers now have to conduct augmented tests and to officially register the new medication.
Source: http://en.rian.ru/analysis/20061024/55089878.html

[Return to top]

Government Sector

27. *October 23, Washington Post* — **As federal spending tightens, contractors seek out new clients.** At a time when federal spending is slowing, state and local governments −− flush with cash from rising property−tax revenue and a generally healthy national economy −− are an increasing target for government contractors. Spending by state and local governments on such projects is projected to reach $54.96 billion in 2008, up from $44.24 billion last year, according to Gartner Inc., a research firm. The first few years after September 11, 2001, when the focus was on national security, contractors invested heavily in selling products and services to the Pentagon or the Department of Homeland Security. Many of those companies earned record profits in the process, but now face the daunting challenge of continuing the growth. That's

difficult to do now that defense IT spending has begun to stall. However, for large federal contractors, the state and local markets can be perplexing with 50 states, 19,000 municipalities and 3,200 counties, each with its own way of doing business. Competition for contracts typically last longer −− 18 to 24 months −− and are generally worth less. But collectively, the competitions are getting larger and attracting wider interest. Also see: "A Shift for Defense Contractors" transcript: http://www.washingtonpost.com/wp−dyn/content/discussion/2006/10/17/DI2006101700580.html
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/22/AR2006102200567.html

28. *October 20, Philadelphia Inquirer* — **In New Jersey, an effort to bolster school security.** New Jersey Governor Jon S. Corzine on Thursday, October 19, took aim at violence in classrooms, announcing a multi−pronged plan to tighten school security. His measures will update state lockdown guidelines, add money for training school police officers, and require New Jersey schools to sign agreements with local police departments formalizing security plans. If legislators grant their approval, schools could also be required to run security drills. Currently New Jersey rules require only that public schools keep emergency plans on file. Schools decide what security measures to put in place. The cornerstones of the plan include school officials signing memorandums with local police; tightening state security guidelines; and, Corzine said, putting additional money into his next budget for training school police officers in state security protocols. Another key point, Corzine said, is making sure students perform emergency drills, just as they carry out fire drills. He already has bipartisan support in the Legislature for the emergency drill initiative, he said. And, school bus drivers will be trained in a "situational awareness" program.
Source: http://www.securityinfowatch.com/online/Standards−and−Legisl ation/9733SIW320

[Return to top]

Emergency Services Sector

29. *October 24, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Weather Outlook: Central and Eastern Pacific: At 5:00 a.m. EDT Tuesday, October 24, Hurricane Paul, with maximum sustained wind speeds near 80 mph, was located about 315 miles south−southwest of Cabo San Lucas, Mexico. There is no threat to the U.S. or any U.S. territories. Earthquake Activity: There was a light (4.0) aftershock on the Island of Hawaii (Big Island) Tuesday morning. The quake was centered three miles north−northeast of Kalaoa and was nine miles deep in the crust. No reports of injuries or damage have been received.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat102406.shtm

30. *October 24, Miami Herald* — **FEMA to help Florida plan for two potential disasters.** Calling Florida the state "most vulnerable" to hurricanes, the Federal Emergency Management Agency (FEMA) announced Monday, October 23, they would spend nearly $4 million to help plan recovery from two nightmare scenarios: a failure of the aging levee around Lake Okeechobee and a Category−5 hurricane slamming Greater Miami. The money will pay for the development of precise, laser−based flood maps around the lake and the hiring of seven

planners to develop strategies aimed at lessening the chaotic process of picking up the pieces −− a hole in disaster planning exposed by the aftermath of Hurricane Katrina in New Orleans last year. The new flood mapping will enhance protection by pinpointing areas in most serious danger and is expected to be completed before next hurricane season. The Miami Category−5 hurricane plan is expected to be completed within the next few years.
Source: http://www.miami.com/mld/miamiherald/news/state/15833012.htm

31. *October 23, Federal Emergency Management Agency* — **Additional assistance approved for Hawaii County.** Individuals, households, and businesses in Hawaii County are now eligible for assistance to help them recover from losses due to the October 15 earthquake. The presidential disaster declaration of October 17 made Hawaii eligible for federal disaster aid to supplement state and local recovery efforts. That declaration was amended Monday, October 23, to include the Individual Assistance program for Hawaii County. Individual Assistance includes grants of funds that can be used for authorized purposes such as temporary housing, home repairs, and replacement of essential household items not covered by insurance.
Source: http://www.fema.gov/news/newsrelease.fema?id=30998

32. *October 23, Associated Press* — **Tennessee plans to update its 911 infrastructure.** Tennesseans may soon be able to send emergency dispatchers photos from an accident scene under plans to modernize the state's 911 infrastructure, officials say. The state's Emergency Communications Board voted recently to begin a statewide project to modernize the infrastructure by linking all of its call centers with a digital network. The project, called "Next Generation 911," will "help emergency workers talk to each other faster and easier," said Lynn Questell, the board's executive director. "It will also make everything more reliable." Although 911 call centers across the state have high−tech, modern equipment, officials said information comes to them over old−fashioned wire telephone lines.
Source: http://www.rctimes.com/apps/pbcs.dll/article?AID=/20061023/NEWS01/610230329/1006/MTCN0301

[Return to top]

Information Technology and Telecommunications Sector

33. *October 24, IDG News Service* — **Sony details battery problems.** Sony has provided greater detail about a battery manufacturing problem that is expected to see the replacement of up to 9.6 million laptop computer battery packs. The problem was first acknowledged in August when Dell issued a recall for 4.1 million batteries and until now had been explained as metallic particles that got into the battery during the manufacturing progress. On Tuesday, October 24, Sony expanded on this and said the particles, believed to be nickel, likely got into the battery during two stages in production: when a groove was created in the battery case and when the electrolyte was poured into the cell. But that alone wouldn't be enough to cause the fires that have been reported by laptop owners. For that to happen, Sony believes that the particles would have to fall into a small triangular gap in the cell body right at the point where the cathode ends between two layers of spacer material. Then, depending on system configuration, the conditions could be right for a fire to start in the battery.
Source: http://www.infoworld.com/article/06/10/24/HNsonydetailsprobl em_1.html

34. *October 24, eWeek* — **Microsoft: Trojan, bot infections high; rootkits low.** New statistics from Microsoft's anti−malware engineering team have confirmed fears that backdoor Trojans and bots present a "significant" threat to Windows users. However, according to data culled from the software maker's security tools, stealth rootkit infections are on the decrease, perhaps due to the addition of anti−rootkit capabilities in security applications. The latest malware infection data, released at the RSA Europe conference in Nice, France, covers the first half of 2006. During that period, Microsoft found more than 43,000 new variants of bots and backdoor Trojans that control millions of hijacked Windows machines in for−profit botnets. Of the 4 million computers cleaned by the company's malicious software removal tool (MSRT), about 50 percent contained at least one backdoor Trojan. While this is a high percentage, Microsoft notes that this is a decrease from the second half of 2005. During that period, the MSRT data showed 68 percent of machines cleaned by the tool contained a backdoor Trojan. Despite increased industry interest in Windows rootkits in 2005, Microsoft found a surprising 50 percent reduction in the attacks, which employ stealthy tricks to maintain an undetectable presence on infected computers. "This is a potential trend that will bear watching," the report said.
Source: http://www.eweek.com/article2/0,1895,2036439,00.asp

35. *October 23, Security Focus* — **Xerox WorkCenter / CopyCenter multiple vulnerabilities.** Xerox WorkCenter / CopyCenter are prone to multiple vulnerabilities. Exploiting these issues can allow remote attackers to trigger a denial−of−service condition in a device. Some of these issues may allow for arbitrary code execution as well, but this is unconfirmed.
Vulnerable: Xerox WorkCenter Pro 90; Xerox WorkCenter Pro 75; Xerox WorkCenter Pro 65; Xerox CopyCenter C90 0; Xerox CopyCenter C75 0; Xerox CopyCenter C65 0.
Solution: Xerox has released an advisory including fixes to address these issues. For more information: http://www.securityfocus.com/bid/17014/references
Source: http://www.securityfocus.com/bid/17014/discuss

36. *October 23, CNET News* — **Autodesk rushes out IE7 compatibility fix.** Autodesk plans to release a patch for two products that aim to remedy compatibility problems with Microsoft's new Internet Explorer 7 (IE7). The "hotfix," or patch targeting a specific issue, will be issued for Autodesk Design Review 2007 and Autodesk Design Web Format (DWF) Viewer 7.0 later this week, said Jennifer Toton, a spokesperson for Autodesk. The applications are for viewing and printing 2D and 3D designs in the Autodesk DWF. Some Autodesk users had complained that their Websites that include DWF files no longer worked in IE7.
Source: http://news.com.com/Autodesk+rushes+out+IE+7+compatibility+fix/2100−1002_3−6128726.html?tag=cd.lede

37. *October 23, USA TODAY* — **Sony recalls 3.5 million more batteries.** Sony and the Consumer Product Safety Commission said late Monday, October 23, that the company will recall nearly 3.5 million additional laptop computer batteries because of fire risks. The new recall involves numerous models of batteries in some Sony, Gateway, Toshiba and Fujitsu laptops. Consumers can check their PC−maker's Website or cpsc.gov. The new recall comes as buyers have returned only a small percentage of the 7 million Sony laptop batteries already recalled, data from computer−makers and analysts suggest.
Source: http://www.usatoday.com/tech/news/2006−10−23−battery−usat_x. htm

38. *October 23, IDG News Service* — **City Wi−Fi coverage put to the test.** Numerous cities around the world, and some rural areas, are building or exploring wireless networks that can deliver fast Internet access everywhere. Even when they don't pay to build the networks, municipalities invest political capital in the promise of connectivity everywhere. Now, a consulting company has launched an independent testing service and is offering to check on the performance of Wi−Fi networks. The service is becoming available as municipal wireless is projected to grow quickly over the next few years. Using a notebook PC with a Global Positioning System and custom software, the consulting company can gather performance data every 100 feet across the advertised service area. Parameters include coverage, data throughput, delay, packet loss and loss of entire files. The company has already tested three networks and found widely varying performances.
Source: http://www.infoworld.com/article/06/10/23/HNcitywifi_1.html

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 4662 (eDonkey2000), 44913 (−−−), 6881 (bittorrent), 37130 (−−−), 65530 (WindowsMite), 25 (smtp), 1027 (icq), 139 (netbios−ssn) 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

39. *October 23, Dowagiac Daily News (MI)* — **Two pipe bombs found in Howard Township, Michigan.** Two pipe bombs were found recently underneath a bridge on Thompson Road in Howard Township, MI. The plastic tubing was about two feet long and stuffed with gunpowder and projectiles. Howard Township Fire Chief Ronald Fazi told the Howard Township board during its monthly meeting last week that the pipe bombs were located by the property owner. The Michigan State Police bomb squad, the township fire department and Southwestern Michigan Community Ambulance Service were called to investigate. Fazi said the pipe bombs were found when the property owner went to look at a deer carcass. Fazi said state police are warning the public that if anything looks like a pipe bomb not to pick it up or handle it at all. He said the end of the pipe was taped shut. Pulling off the tape could have caused an explosion.
Source: http://www.dowagiacnews.com/articles/2006/10/23/news/dnnews2 .txt

40. *October 20, Kansas City Star (MO)* — **Suspicious package blown up in south Kansas City.** Officers in hazardous−material suits inspected a suspicious package near 87th Street and Newton Avenue in Kansas City, MO. Police later blew the package up. Authorities investigating a suspicious package cleared out an apartment complex in south Kansas City on Friday, October 20, and shut down several blocks surrounding 87th Street and Newton Avenue. A maintenance man noticed a box lying on the sidewalk near the Hilltop Village Apartments

about 10 a.m. CDT, said Jeff Lanza, an FBI spokesperson. It was about one foot long, six inches deep and looked like it was some sort of camera case. But there was no reason why the package would have been left out in the open. Kansas City police were called, and they used one of their robots to X−ray the box. The scan showed electronic components and unidentified material inside, which raised suspicions. The police decided to blow open the package. Inside the box, the robot could see a jar and a red plastic bag, both labeled with writing that appeared to be Arabic. The bag contained a black powder, which had started to spill out. The FBI was called to the scene.
Source: http://www.kansascity.com/mld/kansascity/news/breaking_news/ 15810031.htm

[Return to top]

General Sector

41. *October 23, Associated Press* — **Student accused of planting explosives near U.S. Embassy in Venezuela.** Venezuelan police detained a university student outside the U.S. Embassy on Monday, October 23, saying he had planted two pipe bombs nearby. Police closed the street to traffic and set off the two low−intensity explosives, which they said were essentially homemade fireworks. Dozens of children were evacuated from an adjacent school. Nobody was injured. Embassy spokesperson Brian Penn said a motorcycle taxi driver "started screaming" to alert security guards after the youth made a remark to the driver. Local police chief Wilfredo Borraz told reporters that one of the devices was found outside the school and the other in a planter about 50 yards from the embassy entrance. He said both were wrapped in black plastic bags and contained "small fliers with publicity alluding to Hezbollah" −− the Lebanese guerrilla group that recently fought a month−long war with Israel. He said police glimpsed electrical wires protruding from one of the plastic pipes before setting it off. Borraz said the youth's knapsack held materials for making the small explosives, along with a card identifying him as a student of the state−run Bolivarian University −− a school offering free education that was founded by President Hugo Chavez.
Source: http://www.wjla.com/news/stories/1006/370851.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