



Department of Homeland Security Daily Open Source Infrastructure Report for 08 November 2006

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 a United Airlines plane's wing clipped the tail of another jetliner on Tuesday, November 7, as they taxied toward takeoff at Chicago's O'Hare International Airport. (See item [14](#))
- The United Nations' World Health Organization is launching an international taskforce to combat counterfeit medical products, a market that brings in tens of billions of dollars annually as it promotes drug resistant strains of disease, can worsen medical conditions, and may kill its patients. (See item [23](#))
- USA TODAY reports the federal government is working with prisons in dozens of states to improve intelligence gathering and monitoring of inmates in a stepped-up campaign to curb homegrown terrorism behind bars. (See item [39](#))

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. *November 07, Patriot–News (PA)* — **Faulty signal linked to Three Mile Island shutdown.** A signal unintentionally transmitted during testing of a device that measures steam pressure caused the automatic shutdown of Three Mile Island's Unit 1 reactor last week. The reactor

returned to power about 5 p.m. EST Sunday, November 5, after plant engineers identified the problem and corrected it, said Ralph DeSantis, spokesperson for plant operator AmerGen Energy. The episode threw the plant off line for 35 hours. The problem was on the non-nuclear side of the plant and no radiation was released, officials said. Workers were testing a device that measures the pressure of steam coming out of a turbine and into a condenser, where it is converted back into water. The digital readings produced by the instrument during the test were not supposed to be conveyed to the plant's monitoring system, but somehow were, DeSantis said. "We've done it before, but this time [the signal] got through and sent an artificial signal to the brain and it shut the plant down," he said. DeSantis said community officials nearest the plant were notified within minutes of the shutdown. The company also notified the state Department of Environmental Protection and the Pennsylvania Emergency Management Agency.

Source: <http://www.pennlive.com/news/patriotnews/index.ssf?/base/new/s/1162869909236980.xml&coll=1>

2. *November 07, U.S. Energy Information Administration* — **EIA releases November Short-Term Energy Outlook.** The recent announcement of plans for a 1.2 million barrels per day (bbl/d) cut in oil production by the Organization of the Petroleum Exporting Countries (OPEC) has not yet made much of an impact on world oil prices, as the market awaits evidence of substantial compliance. Recent spot prices for West Texas Intermediate (WTI) crude oil are the lowest since February 2005. Demand for petroleum should grow as the winter heating season ramps up. With some reduction in OPEC oil production, the price of WTI crude oil is projected to rise over the next several months. The price of WTI crude oil is projected to average around \$66 per barrel in 2006 and \$65 per barrel in 2007. Our forecast of winter heating fuel expenditures has not changed significantly from last month. Average household heating fuel expenditures are projected to be \$928 this winter compared to \$947 last winter. This is the first winter since the winter of 2001–02 in which home heating fuel expenditures are not expected to significantly increase over the prior winter.

Source: <http://www.eia.doe.gov/steo>

3. *November 06, Associated Press* — **Utility company behind Europe blackout.** A German utility confirmed it caused a weekend outage that left millions of people in several countries without power, but denied Monday, November 6, that the blackout revealed a lack of investment in Europe's power grids. E.ON AG said it switched off a high-voltage transmission line over a German river on Saturday night to allow a newly built Norwegian cruise ship to pass safely. That triggered a blackout that briefly left 10 million people in countries including Germany, France, Italy, and Spain without power. The European Commission said the outage showed the vulnerability of the 25-nation EU without proper management of energy transmissions across national boundaries. "Events in one part of Europe impact on other parts and once again confirm the need for a proper European energy policy," EU Energy Commissioner Andris Piebalgs said. The EU commission had already planned to unveil a major energy security plan in January, and EU spokesperson Tarradellas Espuny said the weekend blackout added urgency to the need for grid operators to develop binding and uniform network security standards. French Prime Minister Dominique de Villepin said that the outage showed the need for a common EU energy policy.

Source: http://seattlepi.nwsource.com/national/1103AP_Europe_Blackout.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. *November 07, Guardian (UK)* — **Online bank fraud up by 55 percent.** Losses from online banking fraud have risen sharply following a surge of nearly 1,500 percent in the number of bogus bank Websites used by criminals to plunder people's accounts, new figures show. Cash machine fraud has also risen by 37 percent, driven by criminals using miniature cameras to spy on people keying in pin numbers, says the Association for Payment Clearing Services (Apacs). But overall, credit and debit card fraud losses have fallen. For the six months to June 30, they were down five percent on the losses recorded during the same period last year. Online banking fraud losses were up 55 percent on losses racked up during the same period last year. These losses involved "phishing" scams. The chip and pin regime has made so-called card-not-present fraud more attractive for scammers. It accounts for almost half of all losses but, even though there has been an explosion in the numbers of people shopping online, this type of fraud grew by only five percent year-on-year, said Apacs. Despite all the headlines about identity theft, credit, and debit card ID fraud fell seven percent over the period.
Source: <http://money.guardian.co.uk/saving/banks/story/0,,1941239,00.html>
5. *November 07, Finextra* — **UK banks prepare to test online shopping authentication system.** UK's Association for Payment Clearing Services (Apacs) is liaising with banks, card schemes, retailers, and systems vendors on the introduction of an authentication system for use in both online and telephone shopping, as the latest fraud figures show rising levels of CNP (card not present) crime. The proposed system would work via a cardholder inserting their chip and PIN card into a hand-held card reader, and entering their PIN. On validating the PIN entered, the reader generates a unique, one-time only passcode, which is relayed to the retailer for authentication with the cardholders bank. Bank-owned Apacs says it will aim to conduct a coordinated trial sometime in 2007. Overseas markets are expected to account for a bigger proportion of card crime, as criminals target countries that have not yet upgraded to the more secure technology. To help tackle this, the European banking industry has set itself the target of completing its chip card rollout by 2010.
Source: <http://finextra.com/fullstory.asp?id=16118>
6. *November 07, Herald Tribune (FL)* — **Comcast warns of phishing scam.** Comcast is warning customers to be on the lookout for phishing e-mails that might look like they came from the cable giant and ask for personal information. The e-mails might contain a Comcast logo.

Customers can forward them to abuse@comcast.net with the subject line "phishing e-mail" so that Comcast can investigate them.

Source: <http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/2006/1107/BUSINESS/611070380>

7. *November 06, Security Focus* — **U.S., Korea top list of phishing hosts.** The United States and South Korea top the list of countries that hosted phishing sites in October, according to data from PhishTank, an open database tracking trends in e-mail fraud attacks. The database, which is run by Internet start-up OpenDNS and collects information from volunteers, confirmed 3,678 valid phishing attacks, about 24 percent of which sent victims to hosts in the U.S. Another 14 percent of phishing attacks referred victims to hosts in South Korea. In total, eleven countries — including India, China, and Brazil — hosted the malicious servers linked to more than three quarters of all phishing attacks in October. On average, the PhishTank community took a little more than 18 minutes to identify a phishing attack. EBay and its subsidiary PayPal were the most targeted organizations, with 73 percent of all attacks in October using those brands to lure users. Almost 80 percent of the phishing attacks included a malicious link using a domain name, while the rest used a numerical Internet address.
- Source: <http://www.securityfocus.com/brief/349>

8. *November 06, Associated Press* — **Mexico City bomb blasts hit court, party HQ, bank.** The Mexican government called for calm Monday, November 6, after homemade bombs blew up at the Federal Electoral Tribunal, a bank branch, and the former ruling party's headquarters in the country's capital. Police deactivated a fourth explosive before it detonated at a second bank branch. There were no injuries and no claims of responsibility for the blasts, which were widely dispersed across Mexico City. The blasts shortly after midnight rattled nerves in Mexico, which has been besieged by protests since its polarizing July 2 presidential elections. Mexico City Public Safety Secretary Joel Ortega said that emergency officials received two telephone calls warning that bombs were about to be detonated. Two explosions at a branch of Canadian-owned Scotiabank in southern Mexico City ripped through the ceiling and shattered windows. Ortega said a police bomb squad deactivated an explosive device at a second branch of Scotiabank near the tribunal. The device, labeled "Bomb Danger," was made with a digital watch, a battery and ammonium nitrate, and fuel oil. In recent years, several small bombs have been placed at bank offices in Mexico. Those explosives were accompanied by messages in which small, radical leftist groups took responsibility.
- Source: <http://edition.cnn.com/2006/WORLD/americas/11/06/mexico.explosions.ap/>

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

Transportation and Border Security Sector

9. *November 07, CBS2 (NY)* — **Fears of onboard explosives center on food services.** Responding to a tip that food carts could be used to bring explosives aboard a plane, CBS2 News went to John F. Kennedy International Airport to investigate. At the LSG Sky Chefs plant where thousands of airline meals are prepared each day, there were gaping holes in security, starting at the entrance to the facility. There the guard checked the license that reporter Scott Weinberger handed him and waved the vehicle in. But the license belonged to a photographer, who looks nothing like Weinberger. Wearing a hidden camera, a CBS 2 photographer walked

through an unlocked door into the Sky Chefs food preparation plant. The next day the photographer walked through the loading bay, where food carts sit before they're placed on waiting trucks. Transportation Security Administration regulations put in place after 9/11 require a representative of the airlines to "conduct a visual inspection of all catering carts." But only an unspecified percentage of trays must be pulled and checked for "signs of tampering and items that do not belong." Yet, two years before 9/11, U.S. Customs agents at Miami Dade Airport arrested numerous Sky Chefs employees for smuggling cocaine in compartments on the carts.

Source: http://webstv.com/investigates/local_story_310163126.html

10. *November 07, Associated Press* — **Northwest Airlines mechanics vote to end 15-month strike.** The 15-month-old mechanics strike against Northwest Airlines Corp. ended on Monday, November 6, with union approval of a new contract. The strike by 1,600 mechanics long ago ceased to have a visible effect on Eagan, MN-based Northwest, which hired permanent replacement workers and outside contractors to replace the mechanics. Seventy-two percent of the members of the Aircraft Mechanics Fraternal Union chose to accept the contract. Replacement workers will keep their jobs. Mechanics who lost their jobs will have the option of being classified as laid off, which allows them to re-apply for positions as they open and retain their seniority for purposes of determining who gets hired back first.

Source: http://www.usatoday.com/travel/flights/2006-11-07-nwa-strike-ends_x.htm

11. *November 07, USA TODAY* — **NYC plane crash was all too typical.** As New York Yankees pitcher Cory Lidle and his flight instructor cruised their small plane over the East River past spectacular views of New York City skyscrapers, they ran into a deadly mix of problems that repeatedly contribute to crashes throughout the country. Lidle's fiery crash last month into the side of a New York high-rise was the most publicized small plane incident in years, but it was typical of fatal accidents that occur four or five times a week and claim hundreds of lives a year, according to a USA TODAY analysis of accident statistics and top safety experts. A preliminary report by federal investigators Friday, November 3, the National Transportation Safety Board (NTSB) reported that wind, coupled with the pilot's inability to turn sharply with only about 1,700 feet of room, forced the aircraft off its intended path over the East River. The numbers of private plane crashes and resulting deaths have fallen dramatically since the 1980s. But in the broader category of all flights except those of air carriers, the fatal accident rate is still more dangerous than other types of flying.

Source: http://www.usatoday.com/news/nation/2006-11-06-small-planes-cover_x.htm

12. *November 07, NewsNet5 (OH)* — **Man arrested taking gun through Ohio airport.** A Warrensville Heights man was arrested Tuesday, November 7, after he was allegedly found with a loaded gun at Cleveland Hopkins International Airport. Arrion Tobbs, 30, was trying to go through a security checkpoint with a loaded .41 caliber handgun in his bag, police said. Cleveland police arrested Tobbs for carrying a concealed weapon.

Source: <http://www.newsnet5.com/news/10264760/detail.html>

13. *November 07, Associated Press* — **New England regional airport traffic drops.** Passenger traffic was down in September for the 12th consecutive month at T.F. Green Airport in Providence, according to the Rhode Island Airport Corp. There were 412,515 passengers for the month, an 11.6 percent drop from 466,835 a year earlier. Airport spokesperson Patti Goldstein

said the trend reflects a drop in daily departures and a switch to smaller planes to cut down on airline fuel costs. The trend appears to be affecting smaller, regional airports more than larger hub cities. New Hampshire's Manchester–Boston Regional Airport reported a 9.8 percent drop for the first eight months of 2006. "Many medium–sized airports nationwide are experiencing similar challenges as airlines reduce capacity and cut costs, trying to return to profitability," Kevin Dillon, director of the Manchester airport, said in a written statement. Also, officials at Bradley International Airport, near Hartford, CT, said passenger traffic through September was down 4.9 percent, compared with the first nine months of last year.

Source: <http://www.concordmonitor.com/apps/pbcs.dll/article?AID=/20061107/REPOSITORY/611070373/1002/NEWS02>

14. *November 07, Associated Press* — **Two planes clip on O'Hare taxiway.** A United Airlines plane's wing clipped the tail of another jetliner Tuesday, November 7, as they taxied toward takeoff at O'Hare International Airport, aviation officials said. No injuries were reported. One of the planes was turning left and the wing of the second plane, another United flight, hit the first plane's tail, said Federal Aviation Administration spokesperson Tony Molinaro. Both flights were canceled, United said on its Website. Chicago Department of Aviation spokesperson Wendy Abrams said the airline was inspecting both aircraft and the Federal Aviation Administration and National Transportation Safety Board were being notified. Flight 672, a Boeing 737, to New York's LaGuardia Airport had 110 passengers and Flight 732, an Airbus 320 en route to Dulles International Airport outside Washington, DC, carried 96 passengers.

Source: <http://www.forbes.com/home/feeds/ap/2006/11/07/ap3152647.htm> 1

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

15. *November 07, USDA Agricultural Research Service* — **Genetics research helps diagnose scrapie disease in sheep.** More accurate genetic tests for diagnosing scrapie disease in sheep have been developed by Agricultural Research Service (ARS) scientists in Clay Center, NE. They believe this achievement will promote scrapie's eventual eradication. Contagious, incurable and fatal, scrapie is the sheep industry's chief disease priority, costing U.S. producers an estimated \$20 million every year. Scrapie's name reflects the disease's most distinctive symptom: an uncontrollable itching sensation that causes afflicted sheep to compulsively scrape their bodies against nearby objects. Most sheep die one to six months after symptoms appear, although they may be infected for years without showing any signs. Drawing from a diverse group of U.S. sheep, researchers in Clay Center have re-sequenced the prion gene, identifying new genetic variation. This achievement has improved commercially available genotyping tests and enhanced the national scrapie eradication program run by the U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

16. *November 06, GovExec* — **DHS officials discuss effects of foot-and-mouth outbreak.** The Department of Homeland Security's (DHS) senior adviser for weapons of mass destruction said late last week that the introduction of foot-and-mouth disease on American soil would have a tremendous effect on the U.S. economy, whether the outbreak is intentional or accidental. Maureen McCarthy, the weapons adviser, on Friday, November 3, told attendees of the Association for Intelligence Officers' annual convention that such an outbreak would cost the American agriculture economy "hundreds of billions" of dollars and could shutter some trade borders for "years" if officials deem it necessary. Acknowledging the potential for disastrous consequences for the agriculture industry and the American economy, Kimothy Smith, DHS chief veterinarian and acting director of national biosurveillance, said that in the event of a foot-and-mouth outbreak, it would be possible to implement import bans on a nation-by-nation basis.

Source: [http://www.govexec.com/story_page.cfm?articleid=35414&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=35414&dcn=to%20daysnews)

17. *November 06, USDA Animal and Plant Health Inspection Service* — **USDA to hold national invasive species, forest health meeting.** The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service and Forest Service, in conjunction with the National Invasive Species Council, invite interested stakeholders to attend the first Invasive Species and Forest Health: Expanding the Team stakeholders meeting Tuesday and Wednesday, November 14–15, in Washington, DC. The goal of the two-day forum is to raise awareness about the growing threat invasive species pose to America's forests, build new partnerships to assess and rapidly respond to these pests, and strengthen existing relationships between stakeholders and officials concerned with the health of U.S. forests. For more information about the Forest Health and Invasive Species: Expanding the Team conference, refer to: <http://www.aphis.usda.gov/ppq/meeting/foresthealth/index.htm> 1
Source: <http://www.aphis.usda.gov/newsroom/content/2006/11/foreshlth.shtml>

[[Return to top](#)]

Food Sector

18. *November 07, Canadian Food Inspection Agency* — **Canada warns of suspected tampering associated with various ham and sliced meat products.** The Canadian Food Inspection Agency and Maple Leaf Foods are warning the public not to consume certain ham and sliced meat products. These products may have been subject to tampering with an unknown contaminant. A small number of syringe casings have been found by employees during the production process. There have been no reported illnesses associated with the consumption of these products and at this time no tampered product has been found at the retail level. Maple Leaf Foods, Kitchener, Ontario is voluntarily recalling the affected products from the marketplace.

Source: http://www.inspection.gc.ca/english/corpaffr/recarapp/2006/2_0061107e.shtml

[[Return to top](#)]

Water Sector

19. *November 07, United Press International* — **Russia warns of terror plot on water infrastructure.** Russian security officials said Tuesday, November 6, they have information terrorists may try to hit hydropower plants in the country's southern regions. Nikolai Patrushev, director of federal security service at the National Anti-Terror Committee, said the Volgograd water reservoir, the Tsimlyanskoye hydropower project, hydropower stations in the Saratov Region and the Dagestan Republic are among those targeted in the plot, reports the Itar-Tass news agency. Patrushev said the current systems in place to protect these facilities are not adequate.
Source: <http://www.upi.com/NewsTrack/view.php?StoryID=20061107-101528-6132r>
20. *November 06, Associated Press* — **Salt water intrusion in Louisiana a threat to paper mill, drinking water.** Salt water in Bayou Lafourche, LA, has forced sporadic shutdowns over the past week of a paper mill that requires large quantities of fresh water for its products. The problem is being blamed on intrusion of Gulf of Mexico water into the ecosystem downstream and a failure of pumps located up the bayou to keep up with fresh water demands for the area. Similar problems more than six years ago were a key reason for construction of a lock that keeps salt water from the Gulf Intracoastal Waterway out of a Lockport canal that feeds into Bayou Lafourche. At that time there were reports of high salt content in drinking water used by residents.
Source: <http://www.leesvilledailyleader.com/articles/2006/11/06/news/news7.txt>

[[Return to top](#)]

Public Health Sector

21. *November 06, National Institutes of Health* — **MRSA toxin acquitted: Study clears suspected key to severe bacterial illness.** Researchers who thought they had identified the bacterial perpetrator of the often severe disease caused by community-associated methicillin-resistant *Staphylococcus aureus* (CA-MRSA) had better keep looking: Scientists at the National Institute of Allergy and Infectious Diseases (NIAID), part of the National Institutes of Health, have exonerated a toxin widely thought to be the guilty party. Pantón-Valentine leukocidin (PVL) is one of many toxins associated with *S. aureus* infection. Because it can be found in virtually all CA-MRSA strains that cause soft-tissue infections, several research groups previously have proposed that PVL is the key virulence factor. But new evidence strongly suggests that is not the case. A study led by NIAID researchers at Rocky Mountain Laboratories in Hamilton, MT, shows that the two major epidemic CA-MRSA strains and the same strains with PVL removed are equally effective at destroying human white blood cells — our primary defense against bacterial infections — and spreading disease. The findings, which appear online in *The Journal of Infectious Diseases*, are surprising because many scientists had presumed that CA-MRSA uses PVL to target and kill specific white blood cells known as neutrophils.
Abstract: <http://www.journals.uchicago.edu/ucp/WebIntegrationServlet?c=all=ContentWeblet&url=http://www.journals.uchicago.edu/JID/journal/issues/v194n12/36574/36574.html?erFrom=40413841970491>

22. *November 04, Xinhua (China)* — **China to conduct TB drug resistance survey in the next two years.** The Chinese Ministry of Health is to conduct a two-year nationwide survey on the spread of tuberculosis (TB) and the effectiveness of drugs being used to combat the potentially fatal disease. Health officials hope the survey will help in the control of TB and its treatment by analyzing factors that lead to drug resistance. A national survey in 2000 showed that 27.8 percent of Chinese TB patients were resistant to at least one of the available drugs, while 10.7 percent were resistant to more than one drug.
Source: http://news.xinhuanet.com/english/2006-11/04/content_5289963.htm
23. *November 02, United Nations* — **UN health agency launches attack on multi-billion-dollar counterfeit medicine market.** The United Nations (UN) health agency and its partners will this month officially launch the first ever international taskforce to combat counterfeit medical products, a market that brings in tens of billions of dollars annually as it promotes drug resistant strains of disease, can worsen medical conditions and may kill its patients. “They are present on all markets and are increasing as counterfeiters’ methods become more sophisticated, infiltrating official channels of distribution as well as using illegal Websites to sell their wares,” the UN World Health Organization (WHO) said Thursday, November 2, in announcing the first meeting in Bonn, Germany, on November 15–16 of the International Medical Products Anti-counterfeiting Taskforce (IMPACT). Unveiling a global plan of action, IMPACT will release the most recent estimates of counterfeit products on the world’s markets, launch pilot programs in three countries, and present a tool to strengthen countries’ legislative capacity to tackle counterfeiting.
For more information on IMPACT: <http://www.who.int/medicines/services/counterfeit/en/>
Source: <http://www.un.org/apps/news/story.asp?NewsID=20462&Cr=who&Cr 1=>
24. *November 02, UK Health Protection Agency* — **Cases of TB rise steeply in UK during 2005.** Cases of Tuberculosis (TB) in England, Wales and Northern Ireland have increased by 10.8 percent from 7,321 cases reported in 2004 to 8,113 in 2005 according to new figures released Thursday, November 2, by the UK's Health Protection Agency. Dr. John Watson, Head of the Respiratory Diseases Department at the Agency, said “Levels of TB have been increasing year on year since the late 1980s. This is, however, the largest increase we have seen in any one year since 1999 when we introduced a new surveillance system which provides us with more detailed information about patterns of TB.” London had the highest proportion of cases in 2005 (43 percent), having increased from 3,129 in 2004 to 3,479 in 2005. The regions with the highest number of new cases were the North West (588 in 2004 to 757 cases in 2005), East Midlands (443 in 2004 to 556 in 2005) and the East of England (395 in 2004 to 483 in 2005).
Source: http://www.hpa.org.uk/hpa/news/articles/press_releases/2006/061102_tb.htm
25. *November 01, Journal of Emerging Infectious Diseases* — **Prophylaxis and treatment of pregnant women for emerging infections and bioterrorism emergencies.** Emerging infectious disease outbreaks and bioterrorism attacks warrant urgent public health and medical responses. Response plans for these events may include use of medications and vaccines for which the effects on pregnant women and fetuses are unknown. Healthcare providers must be able to discuss the benefits and risks of these interventions with their pregnant patients. Recent

experiences with outbreaks of severe acute respiratory syndrome, monkeypox, and anthrax, as well as response planning for bioterrorism and pandemic influenza, illustrate the challenges of making recommendations about treatment and prophylaxis for pregnant women. Understanding the physiology of pregnancy, the factors that influence the teratogenic potential of medications and vaccines, and the infection control measures that may stop an outbreak will aid planners in making recommendations for care of pregnant women during large-scale infectious disease emergencies. Refer to source to view the full text report.

To view other articles in the Journal: <http://www.cdc.gov/ncidod/EID/>

Source: <http://www.cdc.gov/ncidod/EID/vol12no11/06-0618.htm>

26. *October 23, Los Angeles Times* — Concern of new *Clostridium difficile* epidemic strain.

While infections with drug-resistant staph and E. coli have been grabbing headlines and public attention in recent months, a new bacterial threat has quietly emerged. Typically seen in elderly hospitalized patients, the illness has begun popping up in the community at large — specifically among healthy younger people, including children and pregnant women. The bacterium responsible, called *Clostridium difficile*, or C. difficile, has been blamed for recent outbreaks of intestinal infections in about 10 states, as well as Canada and Europe. Patients become ill with frequent bouts of watery diarrhea, fever and abdominal tenderness. In rare cases, the infection can progress to sepsis, colitis and even death. "It's something that is usually acquired in the hospital. But now the concern is that there is a new epidemic strain that is seen outside the hospital," says Dr. Preeta Kutty, an investigator for the federal Centers for Disease Control and Prevention (CDC). The strain, identified as NAP1, appears to be more virulent than its predecessor.

Source: <http://www.latimes.com/features/health/la-he-cdif23oct23.1.2 037456.story>

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

Government Sector

Nothing to report.

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

Emergency Services Sector

27. *November 06, PR Newswire* — Nebraska counties run largest incident response exercise in state's history. A tri-county area in Nebraska conducted a multi-county, multi-jurisdictional exercise known as "Operation Triple Play" to test preparedness and response in the event of a major disaster in the area. The objective of the exercise was to coordinate communications and response not only between Sarpy, Douglas, and Washington counties, but also between multiple agencies that included: Emergency Management, Police, Fire, Metropolitan Medical Response, and the Red Cross, among others. Jim Rogers, Douglas County Assistant Director of Emergency Management, said, "This exercise represents the most extensive test and evaluation of our preparedness and response capability in the state's history." Rogers went on to say, "I am pleased to say that the exercise was very successful and demonstrated the commitment and rapid response of our first responders that help make our region safe."

Source: http://www.earthtimes.org/articles/show/news_press_release.1 6558.shtml

28. *November 06, Federal Computer Week* — **GSA opens emergency response office.** Emergency workers who need General Services Administration (GSA) services in fast-moving disasters have a new resource. GSA announced Monday, November 6, that it has consolidated its emergency procurement services into a new Office of Emergency Response and Recovery (OERR). The office puts all of GSA's emergency resources into one central office for first responders, emergency workers, and recovery teams. GSA Chief of Staff John Phelps will be acting chief emergency response and recovery officer until GSA finds a permanent head for OERR.

Source: <http://fcw.com/article96714-11-06-06-Web>

[[Return to top](#)]

Information Technology and Telecommunications Sector

29. *November 07, Sydney Morning Herald (Australia)* — **Chile arrests four accused of hacking foreign governments' Websites.** Chilean police arrested four suspected computer hackers accused of being part of an international group that has broken into thousands of government Websites around the globe in recent years. Police chief Gerardo Raventos said Monday, November 6, that the group was responsible for "infiltrating" more than 8,000 sites, including some run by the governments of Argentina, Bolivia, Colombia, Peru, Turkey, the United States and Venezuela. Raventos said the suspects even hacked into the NASA Website. The suspects were members of an international hackers group identified as the "Byond" team, and had been under investigation for eight months with the cooperation of authorities in the United States, Israel and several South American countries, Raventos said.

Source: <http://www.smh.com.au/news/breaking-news/chile-arrests-4-accused-of-hacking-foreign-governments39-web-sites/2006/11/07/1162661645862.html>

30. *November 07, Tech Web* — **OS bug project is security wake-up call: Gartner.** A new hacker project that promises to disclose one operating system kernel vulnerability daily hasn't yet come up with any serious bugs, a security company said Tuesday, November 7, but Gartner warned enterprises that the plan constitutes a security wake-up call. Last week, security researcher HD Moore, co-creator of the Metasploit Framework penetration testing tool, began posting one kernel bug each day. In July, Moore ran a similar crusade, dubbed "Month of Browser Bugs" that released more than a score of new browser vulnerabilities, including some for Internet Explorer that were later patched by Microsoft. According to Symantec, Moore's "Month of Kernel Bugs" has not yet put forward any major flaws. So far, Moore and others have posted six vulnerabilities. Although Symantec took a wait-and-see position, research firm Gartner said that the danger level was higher. "[This] is a serious wake-up call about the vulnerability of the most fundamental element of the operating system," said analyst Rich Mogull in a research note posted online. "Begin preparing now for more, and more damaging, attacks against the OS kernel...The incorporation of kernel exploits is a very early indication that the complex exploitation of kernel flaws will be simplified," added Mogull.

Source: <http://www.techweb.com/wire/security/193600339;jsessionid=PYDARNGSP1GT4QSNDLPCKHSCJUNN2JVN>

31.

November 07, Tech Web — **'Stration' worm spawns sneak attacks.** Anti-virus vendors completely missed the fact that the most massive worm attack in months has a secondary payload that has sent millions of pharmaceutical spam messages, a security intelligence company revealed Tuesday, November 7. The Stration worm, also known as WarezoV, has been topic number one for anti-virus firms for almost three months, but until recently they hadn't figured out that the malware kicks into second gear about six hours after it's installed. Then, said VeriSign iDefense, it begins sending massive amounts of spam touting Viagra, Xanax, and Propecia prescription medicines. "Lots of AV vendors have been saying that Stration doesn't have a payload," said Mike La Pilla, an iDefense analyst. "But it does. It just takes six hours. Then it contacts a different domain, downloads a spamming Trojan, and starts sending mail." If a user launches the file attached to the original e-mail, a small Trojan downloader executes, searches out the domain of a remote server, and downloads the Stration/WarezoV worm. Stration, in turn, then replicates by grabbing e-mail addresses off the compromised system. Only later does it seek out a second domain for the spam bot.

Source: <http://www.techweb.com/wire/security/193600350;jsessionid=PYDARNGSP1GT4QSNLPCCKHSCJUNN2JVN>

32. *November 06, Security Focus* — **Microsoft Office embedded shockwave flash object security bypass weakness.** Microsoft Office is prone to a weakness that may allow remote attackers to execute arbitrary script code contained in Shockwave Flash Objects without first requiring confirmation from users. A successful attack may allow attackers to access sensitive information and potentially execute malicious commands on a vulnerable computer. The researcher responsible for discovering this issue has indicated that it presents itself on Windows 2003 SP1, Windows XP Professional Edition SP1 and SP2 running Microsoft Office 2003, and Windows 2000 Professional running Microsoft Office 2003. Other versions may be vulnerable as well.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/18583/info>

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/18583/references>

33. *November 06, CNET News* — **Adobe to donate script code to Mozilla.** Adobe will donate software to run JavaScript programs in the Firefox Web browser, the largest code contribution yet to the open-source Mozilla Foundation. The code will form the basis for a new open-source project called Tamarin, which will be governed and manned by developers from Adobe and Mozilla. Adobe will provide the same software, called the ActionScript Virtual Machine, which it uses to run script code in the Adobe Flash Player 9. This virtual machine is expected to be built into future versions of the Firefox browser by the first half of 2008, said Frank Hecker, the executive director of the Mozilla Foundation.

Source: http://news.com.com/Adobe+to+donate+script+code+to+Mozilla/2100-7344_3-6133052.html?tag=nefd.top

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	1026 (win-rpc), 4662 (eDonkey2000), 15281 (----), 6881

(bittorrent), 1027 (icq), 4672 (eMule), 57715 (----), 25530 (----), 1028 (----), 6346 (gnutella-svc)

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

34. *November 07, Pittsburgh Post-Gazette* — Terror force stands down on Heinz Field break in try. The two young men who tried to break into Heinz Field in Pittsburgh, on Sunday morning, November 5, appear to have been up to nothing more than a college prank. Although the Joint Terrorism Task Force responded to the incident and has been monitoring it after Pittsburgh police arrested the two Carnegie Mellon University students, all indications are that they were not bent on anything nefarious. The FBI and federal prosecutors are no longer involved. City police on Sunday arrested Sudeep Paul, 21, of New York, and Anand Shankar Durvasula, 20, of California, after security guards at the field saw them trying to scale a fence at 1:48 a.m. EST. The FBI and the National Football League (NFL), along with local authorities in every NFL city, have been on heightened alert since a threat to stadiums a few weeks ago that turned out to be a hoax by a Wisconsin man. Before that happened, a stadium break-in would probably not have warranted the attention of the Joint Terrorism Task Force, which is made up of numerous federal, local and state agencies.

Source: <http://www.post-gazette.com/pg/06311/736278-53.stm>

35. *November 07, Fort Worth Star Telegram* — Lights out at fields after wiring is stolen. Adult soccer games are being canceled or rescheduled because of a copper theft last week in Mansfield, TX. Overnight Thursday, November 2, thieves stole copper wiring from most light poles at the Mansfield Sports Complex along with wiring from two scoreboards and a breaker box, police said. That has left the complex without electricity until repairs can be made. Copper has become a hot target for thieves as its value has risen to an all-time high, officials said. Cities and construction crews have taken extra precautions to curb theft, including finding alternative building materials. Belinda Willis, a city spokesperson, said that 46 of the 50 light poles at the complex were damaged and that two-thirds of those had wiring taken. Mansfield police spokesperson Thad Penkala said thieves are seeking copper in less accessible places, including utility poles. "It's kind of dangerous cutting into a light pole you think may not have power, but people are showing that they're willing to risk their lives," he said.

Source: <http://www.dfw.com/mld/dfw/news/local/15949081.htm>

36. *November 07, Enterprise (MA)* — Engineers will check condition of Taunton dam. An underwater dive team and drilling company are being called in to determine the extent of deterioration of the antiquated Morey's Bridge dam, which could cost an estimated \$500,000 to replace. David Murphy, managing partner of Jefferson Development Partners LLC, which owns the dam on Bay Street in Taunton, MA, said the cost of restoration is in the \$500,000 range, but could go higher. Jefferson has hired Pare Corp. of Foxboro, MA, an engineering firm, to analyze the 173-year-old earthen and timber dam to determine the damage and recommend

solutions. The dam has gates that regulate the flow of water from Lake Sabbatia into the Mill River. Jefferson also owns the 173-year-old Whittenton Mills dam downstream on the Mill River, which nearly collapsed in October 2005, threatening to flood the center of the city. With the aid of state and federal funds, the Whittenton Mills dam was replaced with a self-regulating spillway made of three million pounds of rock and boulder and pipes. Taunton Emergency Management Director Richard Ferriera said he's worried what a prolonged rain storm may do to the dam.

Source: <http://enterprise.southofboston.com/articles/2006/11/07/news/news/news12.txt>

37. *November 07, KTVZ (OR)* — **Pipe bomb found in Bend canal, disabled.** Bend police called in the Oregon State Police (OSP) Bomb Squad from Salem on Monday, November 6, to neutralize an unexploded pipe bomb found in a dry Central Oregon Irrigation District canal on the southeast side of town. A surveyor working near the COID canal found what he believed was a homemade pipe bomb, said police Sgt. Ron Taylor. Police responded and found the device in the canal, about 40 feet from the bridge, Taylor said. The apparent bomb consisted of a three-to four-inch section of white PVC pipe, with caps on both ends. One end cap had what appeared to be some burnt cannon fuse sticking out of it, Taylor said. Two OSP Bomb Squad technicians arrived from Salem and the device was "rendered safe" about a half-hour later, Taylor said.

Source: <http://www.ktvz.com/story.cfm?nav=news&storyID=17236>

[[Return to top](#)]

General Sector

38. *November 06, Associated Press* — **California fire forces school evacuations, scorches 600 acres.** A wind-driven wildfire in California scorched more than 600 acres of brush on Monday, November 6, torched an industrial yard, and forced the evacuation of two schools before firefighters gained the upper hand, officials said. The blaze 60 miles east of Los Angeles had threatened 100 homes earlier in the day, but firefighters corralled the fire enough to call off firefighting aircraft within several hours, fire officials said. No injuries were reported. The cause was under investigation. An elementary school and a middle school were evacuated because of the smoke, which was carried by the wind all the way to the coast, about 80 miles away. More than 50 children were evacuated from both schools, a school official said.

Source: <http://www.cnn.com/2006/US/11/06/california.wildfire.ap/index.html>

39. *November 06, USA TODAY* — **Feds eye terrorist recruiting in prisons.** The federal government is working with prisons in dozens of states to improve intelligence gathering and monitoring of inmates in a stepped-up campaign to curb homegrown terrorism behind bars. The FBI and Department of Homeland Security (DHS) are urging prison officials to do more extensive background checks on workers and volunteers who meet with inmates. And members of Congress are looking at possible reforms in prison security as a way to combat the spread of extremist Islamic beliefs. Chief among the concerns is that radical Muslim clerics could have access to prisoners and coerce them with terrorist literature. "It's a concern because we know that violent extremist groups will target people in prisons," said Donald Van Duyn, the FBI's counterterrorism director. The intensified surveillance follows the recent arrests of people alleged to be home-grown terror suspects in London and Canada, which have raised concerns

that the U.S. may be vulnerable to terrorism at the hands of its own citizens. A case in California shows how some U.S. prisons have spawned converts to radical forms of Islam. Members of an extremist group robbed a dozen Los Angeles gas stations in 2005 to raise money to finance terrorist attacks on the United States.

Source: http://www.usatoday.com/news/nation/2006-11-06-terror-prison_s_x.htm

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

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

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.