Department of Homeland Security Daily Open Source Infrastructure Report for 14 November 2006

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

Daily Highlights

- California wind company operators say that within the past year, trespassing and burglaries have increased at the 50,000−acre Altamont Wind Resource Area with thieves cutting and stealing the copper electrical cables used to operate the 5,400 windmills east of Livermore. (See item 1)
- The U.S. Coast Guard began a pilot program on Monday, November 13, that will collect biometric information from illegal migrants interdicted while attempting entry into U.S. territory through the body of water between the Dominican Republic and Puerto Rico known as the Mona Passage. (See item 10)

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 13, Tri−Valley Herald (CA)* — **Copper thefts increasing at wind turbines.** Wind company operators say that within the past year, trespassing and burglaries have increased at the 50,000−acre Altamont Wind Resource Area in California, with thieves cutting and stealing the copper electrical cables used to operate the 5,400 windmills east of Livermore. "It's getting pretty serious out there," said Rick Koebbe of PowerWorks LLC, which operates about 920 windmills in the Altamont. Although prices have drifted down recently from the summer's high

of $3.70 per pound to about $3.32 a pound, some are still willing to break the law for the metal. Last week in Florida, thieves broke into an Orlando Utilities Commission junction box and pulled 10,000 feet of copper wiring from underground pipes. Last month, the National Crime Prevention Council and the Institute of Scrap Recycling Industries partnered to coordinate a law enforcement effort with the institute's 1,425 nationwide scrap recyclers to identify stolen materials and catch thieves. The initiative asked recyclers to require photo identification from sellers and to train employees to identify stolen materials, among other things.
Source: http://www.insidebayarea.com/trivalleyherald/localnews/ci_46 49929

2. *November 13, Ottawa Citizen (Canada)* — **Canada moves to shield oil rigs from attacks.** Officials at Natural Resources Canada are drafting amendments to the federal laws that govern offshore oil and gas platforms to better protect the multibillion−dollar rigs against terrorist attack. Officials are looking at ways to give the regional agencies that oversee the platforms more formal authority over security. The amendments being considered would allow the agencies to issue security−related orders to rig operators and conduct security audits, said Felix Kwamena of Natural Resources Canada's critical energy−infrastructure protection division. They could order rig operators to evacuate the platform in the event of an attack. Natural Resources Canada officials say that existing legislation needs to be updated to address security threats. Security at the offshore rigs is already fairly robust, said Howard Pike of the Canada−Newfoundland Offshore Petroleum Board. Because the platforms are hundreds of miles offshore, access is essentially restricted to helicopter or supply boat, he explained. Visitors to the rig by helicopter are closely screened, as are containers shipped in by supply boat. The consortiums that operate the rigs also have a layer of corporate security in place.
Source: http://www.canada.com/ottawacitizen/news/story.html?id=1713d ad1−49dd−4520−9ccb−ec28c096b648

3. *November 11, Columbus Telegram (NE)* — **Minor fire at Cooper Nuclear Station.** Cooper Nuclear Station, an electric power plant in southeast Nebraska, declared a Notification of Unusual Event on Saturday, November 11, after a small fire started at the plant. The notification was declared because of a fire in an electric terminal box located on the fourth floor of the plant's reactor building. The fire was extinguished within 11 minutes by plant fire brigade who de−energized the terminal box and applied dry chemicals to the fire. A Notification of Unusual Event is declared anytime a fire lasts longer than 10 minutes. A Notification of Unusual Event is defined as unusual events, minor in nature, which have occurred or are in progress, which indicate a potential degradation in the level of safety of the station. The damage was contained to the electric terminal box. There were no injuries and no impact on plant operations.
Source: http://www.columbustelegram.com/articles/2006/11/12/news/new s7cooper.txt

4. *November 08, Platts* — **U.S. industry groups urge caution on winter ULSD, biodiesel blends.** The Petroleum Marketers Association of America and the National Biodiesel Board (NBB) on Wednesday, November 8, asked members to be cautious when blending biodiesel this winter, citing "a combination of challenges" with ultra low sulfur diesel (ULSD) and some biodiesel fuel sampling results. The groups said a national fuel quality testing project, co−funded by NBB and the National Renewable Energy Laboratory, found that half the biodiesel samples pulled between November 2005 and July 2006 "were out of spec on at least one parameter." In addition, one−third of the samples "were out of spec for total glycerin, the

same property that caused issues in Minnesota last year," adding that "NBB views these results as unacceptable." Minnesota in September 2005 became the first US state to mandate biodiesel use, requiring all diesel fuel sold there to include two percent biodiesel in a blend known as B2. However, it had to waive the mandate several times after complaints the fuel was clogging filters, possibly due to high amounts of glycerin. This will be the first winter for extensive ULSD use in the U.S. after the product's federally mandated arrival. More than 90 percent of U.S. diesel output is now ULSD.
Source: http://www.platts.com/Oil/News/6313168.xml?p=Oil/News&sub=Oi l

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *November 13, Government Accountability Office* — **GAO−07−76: Global War On Terrorism: Fiscal Year 2006 Obligation Rates Are Within Funding Levels and Significant Multiyear Procurement Funds Will Likely Remain Available for Use in Fiscal Year 2007 (Report).** Because of broad congressional interest, the Government Accountability Office (GAO) is examining the costs of military operations in support of the Global War on Terrorism (GWOT) under the Comptroller General's authority to conduct evaluations on his own initiative. In September 2005, GAO reported the Department of Defense (DoD) cannot ensure reported GWOT obligations are complete, reliable, and accurate, and recommended improvements. In this report, GAO (1) compared supplemental and annual appropriations identified for GWOT in fiscal year 2006 to the military services' reported obligations as of June 2006 and their cost projections for the remainder of the fiscal year, and (2) examined DoD's efforts to improve the reliability of GWOT obligation data. For this engagement, GAO analyzed fiscal year 2006 GWOT related appropriations and reported obligations, and DoD's corrective actions. Because significant multiyear procurement funds from fiscal year 2006 will likely remain available, GAO suggests Congress require DoD provide year−end data on fund availability and plans for additional funds received or requested. DoD disagreed, noting, among other things, it had already justified its needs. To ensure appropriate transparency, GAO continues to believe Congress needs updated data on DoD's plans.
Highlights: http://www.gao.gov/highlights/d0776high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−76

6. *November 09, Reuters* — **U.S. Air Force needs billions to replace aircraft.** The U.S. Air Force is still debating a supplemental budget request for fiscal 2007 to help pay for the global war on terror, including replacing aircraft lost in battle, a top general said on Thursday, November 9. The Air Force has at least $11 billion in needs that were not included in its base budget, General Ronald Keys, commander of the Air Combat Command, told a group of defense writers. The Air Force turned in a fiscal 2008 budget plan that met the Pentagon's top line goal, but left many equipment needs unfilled, Keys said. All the services are getting a

chance to explain their additional funding needs after Deputy Defense Secretary Gordon England last month urged them to expand their fiscal 2007 supplemental requests to include costs beyond the wars in Iraq and Afghanistan.
Source: http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2006-11-09T183530Z_01_N09403305_RTRIDST_0_ARMS-AIRFORCE.XML&rpc=66&type=qcna

[Return to top]

Banking and Finance Sector

7. *November 13, CNET News* — **With IE 7, green means go for legitimate sites.** Starting early next year, the address bar in Internet Explorer 7 will turn green when surfing to a legitimate Website -- but only in some cases, not all. The colored address bar is designed to be a sign that a specific site can be trusted, giving people the green light to carry out transactions there. It is a weapon in the fight against phishing scams, which use fraudulent Websites. The idea is among the draft guidelines created by the CA Browser Forum, an organization that issues certificates for Websites and major browser makers. Last week, Microsoft decided to adopt that draft version for IE 7, released last month. It plans to add the functionality in January. Initially, only corporations will be able to get the online trust indicator -- a rule that shuts out smaller businesses. A primary concern is to help the targets of online scams, said Markellos Diorinos of Microsoft. There is broad agreement in the industry that Web browsers need a better way to identify trusted sites than the familiar yellow padlock icon which was designed to show that traffic with a Website is encrypted and that a third party certification authority has identified the site.
Source: http://news.com.com/With+IE+7%2C+green+means+go+for+legit+sites/2100-1029_3-6134647.html?tag=nefd.lede

8. *November 10, Orange County Register (CA)* — **Bank account data swiped in gas-station scam.** Hundreds of people had their bank account information compromised when they paid at outside pay pumps at three gas stations in Orange County and one in Torrance, CA, police reported Thursday, November 9. Police suspect that thieves used a device to record account numbers and pin codes onto memory chips from pay-point islands at an ARCO station in Westminster, one in Torrance, and at least one in Costa Mesa, said Detective Sgt. Jim Kingsmill of the Westminster Police Department. The Orange County stations were targeted from September 29 to October 9. The stolen information was later used to craft fake debit cards to fraudulently withdraw up to $502 per ATM transaction at 7-Eleven convenience stores and Wells Fargo ATMs in Las Vegas, Kingsmill said. Sgt. Marty Carver said 440 people who paid with debit cards at two gas stations had bank accounts compromised. Westminster investigators discovered someone had attached a sort of skimming device inside or outside a pay-point ARCO station. Kingsmill said they are looking into groups such as organized-crime networks, which have been linked to similar cases.
Source: http://www.ocregister.com/ocregister/homepage/abox/article_1 350521.php

9. *November 10, InformationWeek* — **Millions of U.S. adults notified of data breaches.** An estimated 49 million U.S. adults have been told over the last three years that their personal information has been lost, stolen, or improperly disclosed, the research firm Harris Interactive

said Friday, November 10. Most of the notifications came from government agencies and financial institutions, according to Harris Interactive's national survey conducted in October. More than one in five adults said some organization had notified them that their personal information was improperly disclosed, translating into about 49 million people, Harris said. Among those adults, 48 percent were notified by a government agency, 29 percent a financial company, and 12 percent by a commercial company. Other organizations that had made notifications included educational institutions, six percent, and healthcare facilities, five percent. Much of the damage suffered by victims was caused by friends and family, stolen wallets or purses, pilfered information from mailboxes or trash containers, and insider theft of personal data by employees of organizations.
Survey: http://www.prnewswire.com/cgi−bin/stories.pl?ACCT=104&STORY=/www/story/11−10−2006/0004471908&EDATE=
Source: http://www.informationweek.com/industries/showArticle.jhtml? articleID=193700714

[Return to top]

Transportation and Border Security Sector

10. *November 13, Department of Homeland Security* — **DHS: U.S. Coast Guard begins biometric collection program to deter illegal entry into U.S. territory by sea.** The Department of Homeland Security (DHS) began a pilot program on Monday, November 13, that will collect biometric information from illegal migrants interdicted while attempting entry into U.S. territory through the body of water between the Dominican Republic and Puerto Rico known as the Mona Passage. The Coast Guard will compare the digital fingerprints and photographs of illegal migrants against the US−VISIT database, which includes information about wanted criminals, immigration violators and those who previously encountered government authorities. Those attempting to illegally enter the United States and its territories are prosecuted under U.S. law in conjunction with bilateral agreements in effect. “Biometrics make it virtually impossible to use forged documents or claim a fraudulent identity,” said Robert Mocny, acting director of the US−VISIT program. “The Coast Guard’s comparison of biometrics collected at sea to those collected through the US−VISIT program will greatly enhance our ability to intercept those who pose a threat to national security.” “The Coast Guard's role in maritime border security is to support the national policy of orderly, safe and legal migration while ensuring safety of life at sea,” said Admiral Thad Allen, the commandant of the Coast Guard.
Source: http://www.dhs.gov/xnews/releases/pr_1163445303682.shtm

11. *November 13, Associated Press* — **Amtrak bracing for Thanksgiving travelers.** Amtrak crews are bracing for the busiest travel period of the year as the nation prepares to mark the Thanksgiving holiday. Along the Northeast corridor, 53 extra trains are being added for the Boston to Washington run. Amtrak expects to handle about 125,000 passengers next Wednesday, November 22. The seven−day Thanksgiving holiday travel period begins next Tuesday and ends on Monday, November 27. Amtrak expects to carry about 600,000 passengers in that time.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=53568

12.

November 13, Navhind Times (India) — **Kuwaiti aircraft flies over no−fly zone in Delhi; Indian airports on alert.** A Kuwait Airways aircraft on Monday, November 13, deviated from its flight path after take−off from the IGI Airport in Delhi and moved towards the no−fly zone approaching the Prime Minister's house, triggering a security scare close on the heels of threats of terror attacks to airports across the country. After the incident, authorities advised all foreign airlines about strict adherence to avoid no−fly zone and depute pilots well versed in English as the pilot of the Kuwaiti airliner was a Mongolian national who was not well equipped with the language, official sources said. The diversion of the Kuwait Airlines flight caused scare among security agencies as it followed a number of recent warnings received by aviation and security agencies about possible terror attacks on vital installations including airports as well as threats of hijack of planes bound for the U.S. or Europe. On Sunday, November 12, there was an urgent advisory to put all airports in the country on high alert following a warning from the U.S. Federal Bureau of Investigation that flights from the country to the United States or Europe could be the targets of terrorists.
Source: http://www.navhindtimes.com/articles.php?Story_ID=111422

13. *November 13, Memphis Business Journal* — **Memphis airport upgrades security.** Memphis International Airport is undergoing one of its largest ever security upgrades. Security checkpoints for passengers as well as baggage screening operations are being redesigned and refurbished with advanced technologies to enhance security at the airport. The upgrades will "result in a safer, more secure, less invasive and more expedited experience for passengers," airport officials said. For security checkpoints, Memphis International is installing four Trace Portal machines which detect explosive residue. The machine is a less−intrusive secondary screening procedure that will help reduce the number of "pat−down" searches and reduce wait time.
Source: http://memphis.bizjournals.com/memphis/stories/2006/11/13/da ily4.html

14. *November 13, Washington Technology* — **Biometric airport ID cards coming to Canada.** Canadian officials said they intend to deploy a new biometric identification card for 120,000 aviation workers at 29 major airports by year's end. Minister of Transport Lawrence Cannon proposed to implement the new Restricted Area Identity Card for airport personnel including flight crews, refuelers, and caterers. Authorized by Transport Canada and the Canadian Air Transport Security Authority, the card will incorporate fingerprints and iris scans, according to a November 10 government news statement. The card is touted as "the world's first−ever dual−biometric airport identification system," because it will use both fingerprint and iris biometrics, the announcement said.
Source: http://www.washingtontechnology.com/news/1_1/daily_news/2970 9−1.html

15. *November 12, USA TODAY* — **Most nations stop retiring pilots at 60.** A pending change in international aviation rules could soon lead to older pilots at the controls of airliners flying within the U.S. Next week, commercial airline pilots in all but four countries will be allowed to continue flying until age 65. In most nations, pilots now must retire at age 60. The International Civil Aviation Organization (ICAO), which sets world aviation standards, issued the policy change two months ago. It cited the lack of evidence that pilots in their 60s are more prone to mistakes than younger pilots, provided they're in good health. Since the beginning of the commercial jet age, airline pilots in the U.S. and most other nations have been required to step down at 60. With the change in the international standard, effective on Thanksgiving Day, only

the U.S., France, Pakistan, and Colombia will hold fast to the age 60 retirement rule. Pilots have fought for years to push the retirement age to 65. But Congress, the courts, and the Federal Aviation Administration have refused to order the change. They argue that economics, not human physiology, underlie the rule. With the ICAO changing the world standard, however, U.S. opponents of the current rule gain a powerful argument for change.
Source: http://www.usatoday.com/travel/flights/2006−11−12−pilots−usa t_x.htm

16. *November 09, Government Accountability Office* — **GAO−07−81R: FAA's Proposed Plan for Implementing a Reliability Centered Maintenance Process for Air Traffic Control Equipment (Correspondence).** The Federal Aviation Administration's (FAA) Air Traffic Organization (ATO) is responsible for maintaining approximately 40,000 pieces of air traffic control equipment, such as radars, navigation beacons, communication systems, and instrument landing systems that are essential to the safe operation of the national airspace system (NAS). Senate Report 109−109, asked the Government Accountability Office (GAO) to analyze FAA's plans to develop a reliability centered maintenance (RCM) process and the impact of these plans. RCM is a data−driven, analytical process used to determine the most value−added maintenance requirements that are needed to keep equipment functioning properly. It requires that data be collected and analyzed on the causes and consequences of failures, in order to determine the maintenance needed to prevent future failures. For example, performance data can be analyzed to determine whether a particular component wears out with age or fails randomly −− key information for deciding the maintenance approach most appropriate for that item. A concern has arisen, in part, because FAA experimented several years ago with a different maintenance process that union officials have criticized as unsafe, and because ATO has not explained its vision of an RCM process.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−81R

17. *November 09, USA TODAY* — **Emirates Airline will be taking cell phone route.** Pending approval by the European Aviation Safety Agency, Emirates Airline expects to have a system installed in the first of its Boeing 777 fleet in January that enables cell phones to operate at minimum power levels that won't interfere with in−flight systems. The system is to be rolled out in 100 of the Dubai−based carrier's aircraft in succeeding months. On the plus side for travelers worried about being trapped next to a yakking cell phone−wielding seatmate, the system allows only five calls to be made from an aircraft at any one time. Only cell phones with international roaming capability will work aloft, and roaming charges, averaging about $3.50 a minute, will apply.
Source: http://www.usatoday.com/travel/flights/2006−11−09−in−flight− cellphones_x.htm

18. *November 08, Department of Homeland Security* — **DHS: Aircraft cargo screening program to begin at Seattle−Tacoma Airport.** The Department of Homeland Security (DHS) will begin testing air cargo screening technologies this fall at the Seattle−Tacoma (Sea−Tac) International Airport as part of its previously announced $30 million Air Cargo Explosives Detection Pilot Program (ACEDPP). The purpose of the Sea−Tac testing is to better understand the technological and operational issues associated with detecting hidden persons or explosives that could be in air cargo. Launched in June 2006 at the San Francisco International Airport, the ACEDPP will provide critical knowledge to help the Transportation Security Administration (TSA) make future decisions on air cargo. The program will also assist in technological research and development planning for the nation's air cargo security infrastructure. DHS is

interested in data that illustrates economic and operational impacts to air carriers from enhanced screening levels. Tests will focus on areas that include assessing the flow of air cargo and how quickly it must be screened. In addition, testing will take place to detect carbon dioxide, which may indicate the presence of a human in cargo. DHS will also seek to determine which types of technologies are most effective at detecting threats placed within commodities. DHS is funding the development of new systems, such as X−ray, that can screen entire pallets at one time to look for explosives.
Source: http://www.dhs.gov/xnews/releases/pr_1163024837806.shtm

[Return to top]

Postal and Shipping Sector

19. *November 13, Associated Press* — **Man who mailed powder to Nancy Pelosi, Jon Stewart due in court.** A man suspected of mailing more than a dozen threatening letters containing white powder to Rep. Nancy Pelosi, Jon Stewart, and other high−profile figures was in custody and awaiting a court appearance. Prosecutors planned to file a criminal complaint against Chad Conrad Castagana, 39, in U.S. District Court in Los Angeles on Monday, November 13. He was arrested Saturday for allegedly conveying false information and sending threats by U.S. mail. Preliminary tests showed the white powder was not hazardous, officials said. The letters, which had fake return addresses, were received by Pelosi, a California Democrat who is in line to become speaker of the House; comedians Stewart and David Letterman; Democratic Senator Charles Schumer of New York; and MSNBC host Keith Olberman.
Source: http://www.usatoday.com/news/nation/2006−11−13−threatening−l etters_x.htm

20. *November 10, Seattle Times* — **Mail drill simulates response to bioterror attack.** In one possible medication−delivery method that government officials tested Saturday, November 11, at about 38,000 households in northeast Seattle neighborhoods, the post office delivered little empty boxes with a flier explaining it's all just a drill. After a real attack, the box would contain antibiotics to counteract anthrax, plague, tularemia or some other deadly bacteria that terrorists might spread. "If there were a bioterrorist attack in Seattle, a large number of people would need medications quickly to keep them from becoming sick," said Dorothy Teeter, interim director of County Public Health. After an actual attack, such deliveries by postal carriers would add to drug distribution by about 12 centers that would be set up in schools, community centers, and other locations in King County.
Source: http://seattletimes.nwsource.com/html/localnews/2003386140_h ealthdrill10m.html

[Return to top]

Agriculture Sector

21. *November 13, USAgNet* — **Federal bioterror record−keeping rules.** Federal bioterrorism rules that govern food include record−keeping requirements for producers who transport and process food or feed. The Food and Drug Administration (FDA) has been phasing in rules since last December. By December 9, the rules will require those facilities with 10 or fewer employees that also meet other requirements to comply by registering their facilities with FDA

and maintaining certain records for a year. The Farm Bureau worked to have certain farms exempted from the requirements. A farm exemption covers grain and oilseed producers who harvest and deliver their own raw commodities to an elevator, feed mill, or processor, according to the American Farm Bureau Federation (AFBF). The same applies to livestock, dairy, and poultry operations that only produce and deliver meat, milk, eggs, or fish to a processor. Farmers who mix, grind, or manufacture feed on their farms are exempt −− if the feed is eaten by animals on that same farm or on another farm under the same ownership, according to AFBF.
Source: http://www.usagnet.com/story−national.php?Id=2368&yr=2006

22. *November 13, USAgNet* — **Comment period for BSE rule extended.** The U.S. Department of Agriculture's Animal and Plant Health Inspection has reopened the comment period for a proposed bovine spongiform encephalopathy (BSE) rule. The proposed rule would remove several restrictions regarding the identification of animals and the processing of ruminant materials from BSE minimal−risk regions, as well as BSE−based restrictions on gelatin derived from bovine hides. The extension gives people interested in commenting about the rule additional time. The new deadline is November 24, 2006.
Source: http://www.usagnet.com/story−national.php?Id=2362&yr=2006

[Return to top]

Food Sector

23. *November 13, Dow Jones* — **South Korea mulls inspections of all U.S. beef imports.** South Korea is considering whether it should inspect all imported U.S. beef to address health concerns, Yonhap News Agency reported Monday, November 13, citing the Ministry of Agriculture and Forestry. The ministry's initial plan was to completely test the first four shipments from the U.S., but afterward do only random testing of five percent of all imports, the report said.
Source: http://www.agriculture.com/ag/futuresource/FutureSourceStoryIndex.jhtml?storyId=72600055

24. *November 12, CBC News (Canada)* — **Salmonella scare sparks Hershey recall.** Hershey Canada has recalled many chocolate bars and baking products, including Hershey bars and Reese's Peanut Butter Cups, because they may be tainted with salmonella. Hershey Canada Inc. and the Canadian Food Inspection Agency (CFIA) released a list on Sunday, November 12, of 25 products they say could be contaminated with the bacteria. Food contaminated with salmonella may not look or smell spoiled, but the bacteria can cause symptoms such as high fever, severe headache, vomiting, nausea, abdominal pain and diarrhea. There have been no reported illnesses associated with the consumption of the candy or chocolate chips on the recall list, the company said.
Canadian Food Inspection Agency alert:
http://www.inspection.gc.ca/english/corpaffr/recarapp/2006/2 0061112e.shtml
Source: http://www.cbc.ca/health/story/2006/11/12/recall.html

25. *November 12, Medical News Today* — **University of Illinois scientist helping processors**

keep E. coli out of meat. A University of Illinois (U of I) professor has discovered that certain solutions used by meat processors to extend shelf life actually do double duty as antimicrobial agents, killing such virulent pathogens as E. coli 0157:H7. That's important because E. coli can be spread via recycled solutions used to tenderize and enhance flavor in steaks, chops, and other cuts of meat, said U of I food science professor Susan Brewer. The problem motivated Brewer to study the process used to inject meat with enhancement solutions before they're offered to consumers. Needle injection has been widely used for decades to tenderize meats, and more recently the fresh−meat industry has adopted the use of enhancement solutions. "With needle injection, organisms that exist on the outside of a piece of meat can get poked down into the meat where they're less likely to be killed if consumers like their meat on the rare side," said Brewer. Brewer and her team of graduate students inserted themselves into the process to learn how contamination was likely to occur and how it could be controlled. The scientists found that some solutions used to extend the shelf life of meat also were effective at killing bacteria.
Source: http://www.medicalnewstoday.com/medicalnews.php?newsid=56458

[Return to top]

Water Sector

26. *November 10, BBC News* — **New technology could remove arsenic from drinking water.** Arsenic−contaminated water can be made drinkable cheaply and simply using tiny crystals related to rust, scientists at Rice University in Texas say. The U.S. team says that particles of iron oxide can bind themselves to large amounts of arsenic in water. When a strong magnet is placed above the particles, they clump together like iron filings and are simple to remove. If confirmed it could help nearly 60 million people in Bangladesh who drink water with dangerous arsenic levels. The researchers from Rice University's Center for Biological and Environmental Nanotechnology report their work in the November 10 issue of Science. Report: http://www.sciencemag.org/cgi/content/full/314/5801/964
Source: http://news.bbc.co.uk/1/hi/world/south_asia/6136970.stm

[Return to top]

Public Health Sector

27. *November 13, Reuters* — **Two more cases of bird flu confirmed in Indonesia.** A two−year−old Indonesian boy has died of bird flu, taking the country's human death toll from the virus to 56, a health ministry official said on Monday, November 13. The toddler from Karawang regency in West Java province had had contact with fowl, the most common method of transmission of the virus. Another health ministry official said a 35−year−old woman from a different part of West Java was also being treated for bird flu in a Jakarta hospital, but it was not clear if she had had any contact with fowl. The two victims are not related, Dr. Muhammad Nadhirin, from the ministry's national bird flu center, told Reuters.
Source: http://www.alertnet.org/thenews/newsdesk/JAK154478.htm

28. *November 13, World Poultry (Netherlands)* — **Egypt reports fresh bird flu infection.** A new outbreak of the H5N1 strain of bird flu has been discovered in Luxor, Egypt, according to the

Egyptian Ministry of Health. The MENA news agency reported that tests on domestic fowl at a local lab showed the samples were positive for the highly pathogenic strain of avian influenza. The area has been quarantined, the birds are being culled and those suspected to have come in close contact with the fowls have been under examination
Source: http://www.worldpoultry.net/ts_wo/worldpoultry.portal/enc/_nfpb/true/tswo_portlet_news_singleeditorschoice1_3_actionOverride/___2Fportlets___2Fts___2Fge___2Fnews_singleeditorschoice1___2Fcontent___2FshowDetailsList/_windowLabel/tswo_portlet_news_singleeditorschoice1_3/tswo_portlet_news_singleeditorschoice1_3id/10508/_desktopLabel/worldpoultry/_pageLabel/tswo__page_news_content/

29. *November 12, ABC News (Australia)* — **Australian nursing home battles unidentified, fatal outbreak.** The Jindalee Aged Care Residence nursing home in Canberra, Australia, is at the center of a deadly respiratory outbreak and says it is working with the Australian Capital Territory Health Department to help control the unidentified illness. The outbreak has claimed the lives of four elderly residents, while a further 43 people are still battling the respiratory infection.
Source: http://www.abc.net.au/news/newsitems/200611/s1786477.htm

30. *November 11, Xinhua (China)* — **China's first human bird flu patient healthy after one year recovery.** The first person to survive the bird flu in China has been given a clean bill of health following medical checks performed on Saturday, November 11, at the Hunan Provincial Children's Hospital. Ten−year−old He Junyao's body functions are all normal, said hospital officials, adding that the disease has not affected the boy's growth.
Source: http://news.xinhuanet.com/english/2006−11/11/content_5317148 .htm

31. *November 10, Center for Infectious Disease Research & Policy (MN)* — **Chinese promise H5N1 samples, deny claim of new strain.** China said Friday, November 10, it would share more avian influenza virus samples, despite reported misuse of some shared previously, and repeated its rejection of a report that a new strain of H5N1 virus has spread through southern China, according to news services. The World Health Organization (WHO) said China is sending 20 H5N1 avian flu virus samples to the U.S. Centers for Disease Control and Prevention. Henk Bekedam, WHO representative in Beijing, said the samples are from 2004 and 2005. China's promise to share more avian flu samples comes on the heels of a WHO apology to China for the misuse of previous samples that the country provided.
Source: http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/nov1006china.html

32. *November 09, Center for Infectious Disease Research & Policy (MN)* — **CDC reports 3,830 West Nile cases this year.** Forty−one states and the District of Columbia have reported a total of 3,830 cases of West Nile virus (WNV) infection, including 119 deaths, so far this year, the Centers for Disease Control and Prevention (CDC) said Thursday, November 9. The numbers signal a bigger epidemic than last year, but much smaller than in the record year of 2003. In 2005 a total of 3,000 cases, including 119 fatal ones, were reported, according to the CDC. The record year for WNV in the United States was 2003, with 9,862 cases, including 264 deaths. In the November 10 issue of Morbidity and Mortality Weekly Report, the CDC says this year's cases include 1,339 that involved neurologic disease (encephalitis, meningitis, or myelitis),

2,324 involving fever but no neurologic disease, and 167 unspecified cases.
WNV activity January 1−November 7, 2006:
http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5544a5.htm
CDC's annual statistics on WNV:
http://www.cdc.gov/ncidod/dvbid/westnile/surv&controlCaseCou nt06_detailed.htm
Source: http://www.cidrap.umn.edu/cidrap/content/other/wnv/news/nov9 06westnile.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

33. *November 13, Federal Computer Week* — **Local officials tap new location−aware and multichannel emergency alert systems to better reach a more mobile citizenry.** Blasting alerts to the public during a major crisis has become more than an exercise in traditional broadcasting technology. Sociology now plays a major role, as state and local officials try to cut through an information overload and tailor citizen−centric alert systems to dispatch messages to mobile phones, e−mail devices and other technologies. Localities are no longer relying exclusively on the Emergency Alert System −− formerly the Emergency Broadcast System −− to signal disaster. Because the public has changed how it communicates and accesses information, local officials are devising a variety of ways to notify people of impending crises, whether those relate to homeland security or natural disasters. A small crop of vendors is rushing forward with technical solutions to help localities better reach citizens. Called mass notification systems (MNS), many of the solutions have materialized as hosted offerings, in which the government pays for an alerting service from a third−party provider. Now that alert systems can deliver messages to a mix of devices, most municipalities want to augment, not replace, traditional media alerts with new MNS technology.
Source: http://www.fcw.com/article96777−11−13−06−Print

34. *November 10, Federal Times* — **IG cites up to $4 million in waste on FEMA trailers.** Poor storage and exposure to storms and floods have lost the Federal Emergency Management Agency (FEMA) between $3 million and $4 million in modular homes, a Department of Homeland Security inspector general report found. FEMA stored almost 1,800 modular homes it purchased after Hurricane Katrina at the Red River Army Depot in Texarkana, TX, IG Richard Skinner said in an October 18 report. They all were left exposed to the elements, and almost one−third of those homes were at least partially damaged because their packaging was not weather−resistant. About 110 homes were damaged beyond repair.
Report: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07−03_Oct06.pdf
Source: http://federaltimes.com/index.php?S=2347123

[Return to top]

Information Technology and Telecommunications Sector

35. *November 13, Information Week* — **Mobile devices provide more opportunities for mischief and theft.** Smartphones and similar devices increasingly are being used by business professionals to store information, tap into customer accounts, and exchange data with the office. The expanded use of mobile devices has caught the interest of criminals and malicious hackers, and several proof−of−concept mobile viruses have emerged in recent months. The growth of Microsoft Windows Mobile 5.0 in the device market also creates new security concerns. Windows Mobile 5.0, released to manufacturers in May, offers more and easier ways to exchange information with back−end servers than previous versions, and it's the first Windows operating system to appear on popular Palm devices. Trojan.Wesber, a proof−of−concept virus for Windows Mobile discovered in September, sends messages from a mobile device via the Short Message Service wireless protocol without the device user's consent, similar to the Redbrowser Trojan reported earlier this year. MSIL.Cxover.A, discovered in March, searches for a device connected to a wireless network, then attempts to establish an ActiveSync connection to the device. If successful, the worm copies itself as a file and disconnects the ActiveSync connection. While there haven't been any public reports of data breaches or other incidents resulting from these viruses, they demonstrate hacker interest in mobile devices.
    Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=193700286

36. *November 11, eWeek* — **Alarm raised for critical Broadcom Wi−Fi driver flaw.** Computer security analysts are raising the alarm for a critical vulnerability in the Broadcom wireless driver embedded in PCs from HP, Dell, Gateway and eMachines. The vulnerability, which was exposed as part of the Month of Kernel Bug project, is a stack−based buffer overflow in the Broadcom BCMWL5.SYS wireless device driver that could be exploited by attackers to take complete control of a Wi−Fi−enabled laptop. The vulnerability is caused by improper handling of 802.11 probe responses containing a long SSID field and can lead to arbitrary kernel−mode code execution. The volunteer Zero Day Emergency Response Team warns that the flaw could be exploited wirelessly if a vulnerable machine is within range of the attacker.
    Source: http://www.eweek.com/article2/0,1895,2056023,00.asp

37. *November 10, CNET News* — **UK outlaws denial−of−service attacks.** A UK law has been passed that makes it an offense to launch denial−of−service attacks, which experts had previously called "a legal gray area." Among the provisions of the Police and Justice Bill 2006, which gained Royal Assent on Wednesday, November 8, is a clause that makes it an offense to impair the operation of any computer system. Other clauses prohibit preventing or hindering access to a program or data held on a computer, or impairing the operation of any program or data held on a computer. The maximum penalty for such cybercrimes has also been increased from five years to 10 years.
    Source: http://news.com.com/U.K.+outlaws+denial−of−service+attacks/2 100−7348_3−6134472.html

38. *November 10, Computer World* — **Mutate, fragment, hide: The new hacker mantra.** Hackers working for criminal gain are using increasingly sophisticated methods to ensure that the malware they develop is hard to detect and remove from infected systems, security researchers warned at this week's Computer Security Institute trade show in Orlando. The most

popular of these approaches involve code mutation techniques designed to evade detection by signature−based malware blocking tools; code fragmentation that makes removal harder; and code concealment via rootkits. Unlike mass−mailing worms such as MS Blaster and SQL Slammer, most of today's malware programs are being designed to stick around undetected for as long as possible on infected systems, said Matthew Williamson, principal researcher at Sana Security Inc. The goal in developing such malware is not to simply infect as many systems as possible but to specifically steal usage information and other data from compromised systems, he said. An increasingly popular way of attempting this is with the use of polymorphic code that constantly mutates. Many malicious hackers also now use "packers" to encrypt malware to evade detection.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004967&source=rss_topic85

39. *November 09, Federal Computer Week* — **DHS forum will bring together cybersecurity products, integrators.** The Department of Homeland Security's (DHS) Science and Technology Directorate is planning to play matchmaker early next year by bringing together systems integrators and government sponsors of information systems projects. The directorate will hold a System Integrator Forum on January 17, 2007. A number of new cybersecurity solutions will be unveiled at the event, which will be held in Arlington, VA. The directorate funded the solutions to help reduce federal and commercial cybersecurity vulnerabilities. Technology solutions on display will include next−generation intrusion−detection and −prevention systems designed to stop zero−day, targeted and internal network attacks; source code analysis solutions to eliminate errors in open−source applications; and secure memory monitoring products.
Source: http://www.fcw.com/article96768−11−09−06−Web

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4662 (eDonkey2000), 2234 (directplay), 1027 (icq), 6881 (bittorrent), 1028 (−−−), 4672 (eMule), 15281 (−−−), 25 (smtp), 445 (microsoft−ds) 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

40. *November 08, NWA News (AR)* — **Break−in investigation reveals ammo cache; bomb squad responds.** A routine call turned into a federal investigation last week when Johnson, AR, police discovered a 21, 350 rounds of ammunition, six hand grenades and 40 ammunition cans inside a local business. The discovery was made on November 2 when Johnson police were investigating a break−in at a business. "When they got there, the owner of the business was

like, Oh, while you're here I want to show you something," said Johnson Public Information Officer John Taylor. " That's when he showed them several ammunition cans that had been stored at the business. He didn't know what it was or how it got there, but thought it looked suspicious." On November 3, the Springdale Bomb Unit removed approximately 40 ammo cans from the business. In the cans were six hand grenades and components for an additional 14 grenades. They also found a tear−gas grenade, blasting caps and other dangerous explosive material. Approximately 21, 350 rounds of ammunition were also found stored in the cans. The bomb unit destroyed some of the items and the hand grenades were dismantled safely. Taylor said the investigation is ongoing and that police have conducted various interviews
Source: http://nwanews.com/nwat/News/46897/

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

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

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

Department of Homeland Security Disclaimer