Department of Homeland Security Daily Open Source Infrastructure Report for 17 November 2006

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

Daily Highlights

- The Associated Press reports that more than two−dozen people were arrested in New York on Wednesday, November 15, in connection with a billion−dollar−a−year gambling ring orchestrated through a Website called Playwithal.com. (See item 10)
- The Associated Press reports a man was arrested at Detroit Metropolitan Airport after officials found him carrying more than $78,000 in cash and a laptop computer containing information about nuclear materials and cyanide. (See item 15)
- The House of Representatives has approved the Animal Enterprise Terrorism Act of 2006, which strengthens the ability of the Department of Justice to prosecute animal rights terrorists who do damage to property or threaten individuals associated with an animal enterprise. (See item 23)

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 15, Agence France−Press* — **OPEC slightly increases estimate of world oil demand.** The Organization of the Petroleum Exporting Countries (OPEC) has increased its forecasts for world oil demand this year and said that its recent production cut had succeeded in

stabilizing prices. The forecast and comments by the cartel in its monthly report came amid speculation about whether the 11−member organization would further reduce its output quota at its next meeting in December. OPEC slightly increased its estimate of worldwide demand for oil in 2006, now expected to average 84.3 million barrels per day (bdp), the cartel said Wednesday, November 15. The estimate is an upwards revision of 100,000 bpd from a previous forecast of 84.2 million bpd. In 2007, demand was expected "to grow at a moderate rate of 1.3 million bpd or 1.6 percent," the OPEC report said. In Wednesday's report, OPEC said that a production cut which took effect at the start of the month "appears to have largely achieved its purpose of stabilizing markets and arresting the sharp fall in prices seen the last few months." OPEC said "ample global supplies and calmer geopolitical trends caused oil prices to fall sharply in October."
Source: http://news.yahoo.com/s/afp/20061115/bs_afp/opecenergyoil_06 1115152425

2. *November 14, Associated Press* — **ConocoPhillips cleaning oil pipelines more often.** ConocoPhillips has stepped up its efforts to prevent corrosion−related leaks in its pipelines in the Kuparuk oil field on Alaska's North Slope. The move comes after leaks in pipelines earlier this year damaged the reputation of BP PLC, operator of the Prudhoe Bay oil field, the nation's largest. Kuparuk is the nation's third−largest oil field. Until recently, Conoco ran cleaning pigs through a key network of large Kuparuk pipelines every six months. Beginning in June, the company switched to a monthly pigging schedule and went to a "more aggressive" type of pig to better scrape sediment or other solid material out of the pipes. In two reports provided to federal pipeline regulators, Conoco indicated that it had stepped up pigging in the main pipeline network within the Kuparuk field. Inspection of other pipelines also increased. The reports say no serious corrosion has been found in Conoco−run pipelines. Using other technology, Conoco said it found 12 bad spots in Kuraruk's oil system pipeline network. The worst involved a 43 percent wall thickness loss, which is not considered dangerous by industry standards.
Source: http://ap.alaskajournal.com/stories/state/ak/20061114/120295 048.shtml

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *November 16, Associated Press* — **Toxic spill in California leads to traffic nightmare.** Seven people were evacuated by paramedics from the Foothill Freeway after a collision between two big rigs in Sunland, CA, that spilled hazardous materials all over the road. Fire officials say three of the evacuees were hospitalized with complaints of minor respiratory irritation. No injuries were reported as a direct result of the collision. Officials closed a portion of the 210 Freeway near La Tuna Canyon, where the wreck occurred Thursday morning, November 16.
Source: http://www.kesq.com/Global/story.asp?S=5690780

4. *November 16, Associated Press* — **Rear−ended car hits fuel tanker, setting off explosion on Florida I−75; one dead.** A chain−reaction crash sent a car slamming into a tanker carrying 8,000 gallons of fuel, setting off an explosion on Interstate 75 and killing the car's driver in near Tampa, FL. The crash started when a pickup truck rear−ended the car, which then hit the side of the passing tanker truck Wednesday, November 15. The tanker's driver was able to escape before the vehicle exploded. The stretch of interstate where the crash happened was closed for more than four hours while fire crews let the blaze burn out.

Source: http://kutv.com/nationalwire/TankerFire_a_a_−−−−−/resources_news_html

5. *November 16, WSB−TV (GA)* — **Two−block area near Georgia Tech campus evacuated due to propane leak.** Streets near the Georgia Tech campus have reopened after a leaking propane tank was repaired. Both 10th and State Streets were shut down for about 45 minutes while crews made the repairs. A two−block area around the tank was evacuated during the incident.
Source: http://www.wsbtv.com/news/10335201/detail.html

6. *November 16, Chicago Tribune* — **School closed after hazardous materials found nearby.** Classes were canceled Thursday, November 16, at Prairie Hill Middle School in northwest suburban Cary, IL, after hazardous materials were discovered in a nearby home. "Some sort of hazardous materials were found in the house," Assistant Principal Kevin Ryan said. "Because the house is near the main entrance (of the school), the school has been closed for the safety of the children and parents who would be dropping them off." The school's 820 5th− and 6th−graders were notified of the closure Thursday morning.
Source: http://www.chicagotribune.com/news/custom/newsroom/chi−061116cary−school,1,5264989.story?coll=chi−news−hed

7. *November 16, WTHR (IN)* — **Chemical spill closes I−65 near Lowell, Indiana.** Police closed Interstate 65 near Lowell, IN, because of a chemical leak that caused several injuries. The chemical, sodium hydrosulfite, apparently leaked out of a semi trailer at a truck stop at the intersection of I−65 and Indiana route 2 at the 240 mile marker. Five people were treated for respiratory discomfort.
Source: http://www.wthr.com/Global/story.asp?S=5691626

[Return to top]

Defense Industrial Base Sector

8. *November 16, Government Accountability Office* — **GAO−07−229T: Defense Business Transformation: A Comprehensive Plan, Integrated Efforts, and Sustained Leadership Are Needed to Assure Success (Testimony).** Of the 26 areas on the Government Accountability Office's (GAO) high−risk list of federal programs or activities that are at risk for waste, fraud, abuse, or mismanagement, eight are Department of Defense (DoD) programs or operations and another six are governmentwide high−risk areas that also apply to DoD. These high−risk areas relate to most of DoD’s major business operations. DoD’s failure to effectively resolve these high−risk areas has resulted in billions of dollars of waste each year, ineffective performance, and inadequate accountability. At a time when DoD is competing for resources in an increasingly fiscally constrained environment, it is critically important that DoD get the most from every defense dollar. DoD has taken several positive steps and devoted substantial resources toward establishing key management structures and processes to successfully transform its business operations and address its high−risk areas, but overall progress by area varies widely and huge challenges remain. This testimony addresses DoD’s efforts to (1) develop a comprehensive, integrated, enterprisewide business transformation plan and its related leadership approach and (2) comply with legislation that addresses business systems modernization and improving financial management accountability. The testimony also

addresses two sections included in recent legislation and other DoD high−risk areas.
Highlights: http://www.gao.gov/highlights/d07229thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−229T

9. *November 15, U.S. Department of Defense* — **DoD releases Selected Acquisition Reports.** The Department of Defense (DoD) has released details on major defense acquisition program cost, schedule, and performance changes since the June 2006 reporting period. This information is based on the Selected Acquisition Reports (SARs) submitted to the Congress for the September 2006 reporting period. SARs summarize the latest estimates of cost, schedule, and performance status. These reports are prepared annually in conjunction with the President's budget. The current estimate of program acquisition cost for programs covered by SARs for the prior reporting period (June 2006) was $1,612,605.8 million. After subtracting the cost for one final report (Active Electronically Scanned Array) and adding the costs for one new program (C−5 Avionics Modernization Program) from the June 2006 reporting period, the adjusted current estimate of program acquisition costs was $1,612,885.2 million. For the September 2006 reporting period, there was a net cost increase of $4,824.9 million (+0.3 percent), due primarily to revised cost estimates for the Global Hawk and the Chemical Demilitarization−Assembled Chemical Weapons Alternatives programs.
SAR Program Acquisition Cost Summary as of September 30:
http://www.defenselink.mil/news/Nov2006/d20061115SARs.pdf
Source: http://www.defenselink.mil/Releases/Release.aspx?ReleaseID=1 0188

[Return to top]

Banking and Finance Sector

10. *November 15, Associated Press* — **New York police arrest billion dollar gambling ring.** More than two−dozen people were charged Wednesday, November 15, in connection with a billion−dollar−a−year gambling ring that rivaled casino sports books. The illegal betting scheme was orchestrated through a Website called Playwithal.com, run by the poker player, James Giordano, according to Police Commissioner Raymond Kelly and Attorney Richard Brown. Giordano was arrested, as was Frank Falzarano, a scout for the Washington Nationals. He allegedly was a top earner in a network of 2,000 bookies who took more than $3.3 billion in cash wagers since 2004 from tens of thousands of customers nationwide. "This is the largest illegal gambling operation we have ever encountered," Kelly said. "It rivals casinos for the amount of betting." Though the gambling ring relied on a Website, it was different from the online betting operations targeted by recent federal legislation. The scheme involved placing sports bets through bookies, who would assign bettors a secret code to track their wagers and monitor point spreads and results through the secured Website. The defendants allegedly laundered and stashed away "untold millions of dollars" using shell corporations and bank accounts in Central America, the Caribbean, Switzerland, Hong Kong, and elsewhere, Brown said.
Source: http://news.yahoo.com/s/ap/20061115/ap_on_re_us/internet_gam bling_arrests_6

11. *November 15, IDG News Service* — **Humans called weak link in tech security.** The SANS Institute has some controversial advice for computer security professionals looking to lock down their networks: spear−phish your employees. That's what the U.S. Military Academy at

West Point did in 2004 to a group of 512 cadets, selected for a test. The cadets were sent a bogus e−mail that looked like it came from a fictional colonel, who claimed to be with the academy's Office of the Commandant. More than 80 percent of the cadets clicked on the phishing link. Even after hours of computer security instruction, 90 percent of freshmen cadets still clicked on the link. Because these attacks rely on cooperation from their victims, it's hard to prevent them, said Alan Paller, director of research with SANS. "The only defense against spear phishing is to run experiments on your employees and embarrass them," he said. Paller's organization compiles an annual report on the top to Internet security targets. This year "human vulnerabilities" will make their first appearance on a list. That's because the human factor is being exploited in a growing number of targeted attacks as more and more online criminals come online in Eastern Europe and Asia, Paller said.
Source: http://news.yahoo.com/s/pcworld/20061115/tc_pcworld/127889

12. *November 15, Websense Security Labs* — **Central National Bank of Enid, Fake Bank: McLloyds Bank International, First Exchange Bank, State Bank of India.** Websense Security Labs has received reports of phishing attacks that target bank customers. For each phishing attack below, an e−mail provides a link to a phishing site that attempts to collect personal and account information.
State Bank of India: Users receive a spoofed e−mail message, which claims that banking information needs to be updated because of an upgrade to the servers.
First Exchange Bank (WV): Users receive a spoofed e−mail message, which claims that they have been selected for random verification and must verify their identity.
McLloyds Bank International (fake bank): Users receive a spoofed e−mail message, which lures users into visiting the fraudulent Website.
Central National Bank of Enid (OK): Users receive a spoofed e−mail message, which claims that in order to receive a $100 credit to their account they need to take a quick online survey.
Source: http://www.websensesecuritylabs.com/

13. *November 15, Guardian (UK)* — **Cash machines were bugged with MP3s in scam.** A man who used MP3 players to bug cash machines and steal the personal details of unsuspecting bank customers has been jailed for 32 months. The sophisticated technical scam secured data that enabled Maxwell Parsons's accomplices to use cloned credit cards to buy hundreds of thousands of goods in high−street shops. The scheme, put into action before chip and pin cards were introduced, is thought to have been the first of its kind to be used in the UK. Parsons and his team attached MP3 players to the backs of free−standing cash machines in bars, bingo halls, and bowling alleys. The players then recorded customers' data as it was read on their cash cards and transmitted via a telephone line to banks. Technology imported from Ukraine was used to decode the tones from the transactions and turn them into information which could be used to clone new credit cards.
Source: http://money.guardian.co.uk/news_/story/0,,1948027,00.html

14. *November 15, PC World* — **Phishers take weekends off.** According to research by Symantec, there is over a 30 percent dip in the number of new phishing sites on weekends. "That indicates that phishers are working phishing as their regular job," according to Oliver Friedrichs, of Symantec's Security Response team. So now we're dealing with 9−to−5, punch−the−clock criminal enterprise. Prevention is challenging to say the least. These criminals know what they are doing, and they limit their exposure. "The average life cycle of a phishing site is four

hours," says Friedrichs.
Source: http://blogs.pcworld.com/staffblog/archives/003156.html

[Return to top]

Transportation and Border Security Sector

15. *November 16, Associated Press* — **Airport arrest turns up nuclear info.** A man was arrested at Detroit Metropolitan Airport after officials say they found him carrying more than $78,000 in cash and a laptop computer containing information about nuclear materials and cyanide. Sisayehiticha Dinssa, an unemployed U.S. citizen, was arrested Tuesday, November 14, after a dog caught the scent of narcotics on cash he was carrying, according to an affidavit filed in court. When agents asked him if he had any cash to declare, he said he had $18,000, authorities said. But when agents checked his luggage, they found an additional $59,000. At a court hearing Wednesday, Dinssa was ordered held in custody until at least until Monday at the request of prosecutors. Assistant U.S. Attorney Leonid Feller argued Dinssa was a potential risk to the community and federal agents want to get a warrant to search his computer more thoroughly, Dinssa, who is from Dallas, arrived in Detroit from Nigeria by way of Amsterdam and was headed for Phoenix,
Source: http://www.usatoday.com/news/nation/2006−11−16−airport−nucle ar_x.htm

16. *November 16, Bay City News (CA)* — **Report: security compromised at SFO.** Transportation Security Administration (TSA) officials at San Francisco International Airport (SFO) tipped off airport screeners to impending undercover tests in 2003 and 2004, according to a report released on Thursday, November 16, by the inspector general of the Department of Homeland Security. The report from Inspector General Richard Skinner concluded that TSA officials "covered up known security breaches at SFO and compromised Office of Inspector General covert security testing." In 2005, a former manager with Covenant Aviation Security, a private firm that screens passengers at SFO, reported that he was instructed to alert screeners in advance of covert tests. The inspector general's report confirmed the allegation that TSA and Covenant officials tracked undercover testers, on security cameras and on foot, as the testers moved through the airport, and notified screeners before the testers arrived at checkpoints. The inspector general's office also identified one security breach at SFO that TSA officials did not report, but it concluded that there was no evidence management intentionally covered up or falsified security incidents.
Review of Allegations Regarding San Francisco International Airport, OIG−07−04:
http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07−04_Oct06.pdf
Source: http://cbs5.com/localwire/localfsnews/bcn/2006/11/16/n/HeadlineNews/TSA−REPORT/resources_bcn_html

17. *November 16, WABC−TV (NY)* — **Stewart International may become major airport.** The Port Authority of New York and New Jersey will officially begin the process of turning Stewart International Airport in Orange County into New York's fourth major jetport. The agency's board will vote to authorize its staff to determine legally what the Port Authority would have to do to enhance and operate the former Air Force base, located in Newburgh about 55 miles north of New York City. Currently, the airport is owned by the State of New York. It is the nation's first privatized commercial airport and operates under a 99−year lease agreement between

British transportation company National Express Group and the New York State Department of Transportation. National Express has began soliciting offers for the remainder of its lease. The Port Authority is authorizing funds to begin in−depth studies of what it would need to do to upgrade and operate the facility. Sale of Stewart to the Port Authority would ultimately be a decision made by National Express. A Spanish company is rumored to be interested in purchasing the airport as well.
Source: http://abclocal.go.com/wabc/story?section=local&id=4768314

18. *November 16, Boston Globe* — **Massport board approves $46 million in airport projects.** The Massachusetts Port Authority (Massport) board has approved nearly $46 million in airport construction and renovation projects, including a $26.5 million project to reconfigure aircraft taxiways in the southwest corner of Boston's Logan airfield next year. The taxiway work, which could reduce a recent spate of "runway incursions" when planes violate minimum safe spacing distances, will be funded by the Federal Aviation Administration (FAA) and by proceeds from the $4.50−per−ticket passenger facilities charge Logan passengers already pay. Massport capital programs director Sam Sleiman said, "The project will enhance safety. It's been supported by chief pilots" of airlines serving Logan, "the FAA, and all the aviation community." Massport hasn't chosen a construction contractor, and it's not clear what, if any, delays the construction could cause when work begins next year.
Source: http://www.boston.com/business/ticker/2006/11/massport_board_2.html

19. *November 16, Arizona Central/Wall Street Journal* — **Putting air bags on airplanes.** With tougher safety standards for airplane cabins looming on the horizon, the aviation industry is turning to air bags. Built into specially equipped seatbelts, these air bags explode outward in the event of a sudden impact, cushioning passengers from smacking their heads or torsos against seat dividers, bulkheads, galleys, lavatories, and other potentially hazardous obstructions. Because the air bags expand away from occupants, proponents say, there is less likelihood of injuries from the explosive force of the bag opening than in an auto. The air bags, which are already used in thousands of small planes, aren't intended for use on every seat on a jetliner. They're designed for seats in which passengers are at the greatest risk during a survivable crash −− the small percentage of seats nearest potentially hazardous obstructions or those that turn into lie−flat beds and are angled to face aisles. The impetus for air bags comes from research that determined that in many airline crashes, the actual impact was survivable. After more than 15 years of debate and resistance from airlines, the Federal Aviation Administration ruled that by November 2009 certain seats on existing airliners must be upgraded and all new planes must be equipped with more crash−resistant seats throughout.
Source: http://www.azcentral.com/news/articles/1116wsj−airplane−airb ags16−ON.html

20. *November 15, National Journal's Technology Daily* — **Inspector general outlines flaws in border security plan.** An estimated $2 billion program for border security faces numerous financial and management risks similar to those that doomed past border security efforts, Department of Homeland Security (DHS) Inspector General (IG) Richard Skinner said Wednesday, November 15, in prepared testimony. The department has not adequately defined the operational requirements and acquisition baseline for the initial phases of the Secure Border Initiative (SBInet). SBInet is intended to gain control of the nation's borders by integrating technology, personnel, infrastructure, and processes. DHS Secretary Michael Chertoff has said he believes the department can achieve operational control of the borders by 2008. Skinner,

however, said SBInet is vulnerable to changing schedule and cost estimates. "Until the department fully defines, validates and stabilizes the operational requirements underlying the SBInet program, the program's objectives are at risk, and effective cost and schedule control are precluded," Skinner wrote. He added, "The absence of an acquisition program baseline is a significant risk to the success of the SBInet program." Skinner noted that previous programs to achieve border security, such as the Integrated Surveillance Intelligence System and America's Shield Initiative, failed due to improper management.
IG congressional testimonies: http://www.dhs.gov/xoig/rpts/gc_1163620428568.shtm
Risk Management Advisory for the SBInet Program Initiation, OIG−07−07:
http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07−07_Nov06.pdf
Source: http://www.govexec.com/dailyfed/1106/111506tdpm1.htm

[Return to top]

Postal and Shipping Sector

21. *November 16, DM News* — **Revenue, fuel costs soar for USPS.** Record levels of revenue and volume helped the U.S. Postal Service (USPS) conclude its 2006 fiscal year with net income of $900 million, but increases in fuel and labor costs limited the financial success. The FY 2006 year−end financial figures were released November15, by H. Glen Walker, USPS chief financial officer and executive vice president, during the November meeting of the Board of Governors in Washington, DC. Fuel and transportation costs totaled about $1.7 billion in FY 2006, or $260 million more than anticipated, Walker said. As one of the nation's largest transportation and delivery organizations, the USPS is sensitive to changing energy costs.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/39023.html

22. *November 15, Fulton Sun (MO)* — **Second anthrax hoax puts Missouri emergency officials on alert.** For the second day in a row, local fire and sheriff's officials responded to the Fulton Reception and Diagnostic Center (FRDC) for another possible anthrax scare. The Fulton Fire Department −− with mutual assistance from the Cole County Regional Hazardous Materials Team and the Callaway County Sheriff's Department −− stood in wait early Tuesday morning, November 14, after a suspicious white powder substance was found in a package with a letter discovered in the facility's mailroom. The same emergency units responded to a similar incident Monday at the minimum−security facility −− which involved a substance proven by Hazmat personnel to be crushed aspirin. Tuesday's incident appeared to be a carbon copy of Monday's event −− except the substance found the second time was 95 percent crushed cereal combined with a small amount of aspirin. “I haven't seen the letter. It's currently being processed as evidence by our investigators,” FRDC superintendent Stuart Epps said shortly after the incident occurred. “It's unknown how long that process might take.
Source: http://www.fultonsun.com/articles/2006/11/15/news/046news03. txt

[Return to top]

Agriculture Sector

23.

November 15, Wisconsin Ag Connection — **Animal terrorism act approved by Congress.** A measure designed to give federal authorities the ability to arrest and prosecute animal terrorists who use intimidation, threats and other tactics is expected to be signed by President Bush this month. On Monday, November 13, the U.S. House of Representatives approved the Animal Enterprise Terrorism Act of 2006 −− which strengthens the ability of the Department of Justice to prosecute animal rights terrorists who do damage to property or threaten individuals associated with an animal enterprise. "Animal rights extremists have escalated their attacks on farmers, including harassment, to the point where animal rights terrorism is now one of the top domestic terrorist threats," said WFBF spokesperson Tom Thieding. "This legislation would give law enforcement expanded legal options to catch and prosecute those who threaten the lives of farmers and ranchers and the animals they raise, and not wait for actual damage to take place."
Source: http://www.illinoisagconnection.com/story−regional.php?tble= WI2006&ID=1355

24. *November 14, Animal and Plant Health Inspection Service* — **USDA modifies restrictions regarding the movement of live fish susceptible to viral hemorrhagic septicemia.** The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) modified Tuesday, November 14, an October 24, 2006, emergency order prohibiting the importation of 37 species of live fish from two Canadian provinces into the U.S. and the interstate movement of the same species from the eight states bordering the Great Lakes. These modifications will allow Illinois, Indiana, Michigan, Minnesota, New York, Ohio, Pennsylvania and Wisconsin to move interstate live species of fish susceptible to viral hemorrhagic septicemia (VHS) if they can meet certain conditions designed to prevent the spread of the disease, which isn't harmful to people but can be deadly to fish. With the exception of salmonids, the movement of susceptible species of live fish from Quebec and Ontario into the U.S. remain prohibited under the revised Federal Order. APHIS will be drafting an interim rule to further address the movement of fish from Canada and the Great Lakes states. Under the revised Federal Order, conditions for the interstate movement of VHS−susceptible species vary depending on whether the live fish are being transported for slaughter, research, or other purposes.
Source: http://www.aphis.usda.gov/newsroom/content/2006/11/vhs.shtml

[Return to top]

Food Sector

25. *November 15, U.S. Department of Agriculture* — **USDA announces $39 million to promote U.S. food and agricultural products overseas.** The U.S. Department of Agriculture's Foreign Agricultural Service Wednesday, November 15, announced fiscal year 2006 allocations of $39 million to 56 U.S. trade organizations to promote U.S. agricultural products overseas. "Developing overseas markets is critical to American agriculture," said Agriculture Secretary Mike Johanns. "These programs support U.S. producer associations so they can tap into market opportunities. Agricultural exports support not only the food and agriculture sectors, but the economy as a whole."
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB/.cmd/ad/.ar/sa.retrievecontent/.c/6_2_1UH/.ce/7_2_5JM/.p/5_2_4TQ/.d/1/_th/J_2_9D/_s.7_0_A/7_0_1OB?PC_7_2_5JM_contentid=2006%2F

11%2F0445.xml&PC_7_2_5JM_parentnav=LATEST_RELEASES&PC_7_2_5JM_navid=NEWS_RELEASE#7_2_5JM

26. *November 15, CBC News (Canada)* — **Chocolate−coated almonds added to Hershey recall.** Hershey Canada is adding chocolate−coated almonds purchased in bulk at its factory store in Smiths Falls, Ontario, to its list of recalled products. The chocolate−coated almonds were sold between October 23 and November 10 at the Hershey Chocolate Shoppe. They were not packaged in Halloween, Christmas, or other gift packages. The company, which employs 500 workers in the eastern Ontario town, shut down production and issued a recall of 25 products after a routine inspection inside the plant detected salmonella on November 9. The Canadian Food Inspection Agency said the plant will remain closed until an investigation has been completed.
Source: http://www.cbc.ca/health/story/2006/11/15/hershey−recall.htm l

27. *November 15, Sacramento Business Journal* — **Cantaloupes being recalled by distributor.** Timco Worldwide Inc., announced a voluntary recall on its Sundia brand cantaloupes Wednesday, November 15, saying the melons potentially are contaminated with salmonella. Timco said 504 cartons of the melons, which were grown in Mexico, were distributed in Phoenix, AZ, Colorado Springs, CO, Dallas, TX, and Okeechobee, FL, between October 30 and November 6. Routine sampling of the products, conducted at the border by the U.S. Food and Drug Administration, showed the presence of the salmonella organism in a portion of the cantaloupes.
Source: http://sacramento.bizjournals.com/sacramento/stories/2006/11/13/daily26.html?t=printable

28. *November 15, CBS3−TV (PA)* — **Doctor develops new way to detect E. coli.** Dr. Raj Matharason at Drexel University has developed a test that detects several types of E. coli in just 10 minutes. Currently it takes about 24 hours to test for E. coli, making it difficult to quickly contain an outbreak. With Raj's technology, when food samples are contaminated with E. coli, a sensor is activated and shows up with a downward spike on a computer. The technology will probably first be used by food packagers to test food before it reaches store shelves, but researchers are also working on a small and affordable portable device that people could use in their own kitchens to test food. There is widespread interest in the E. coli test. The Department of Homeland Security is sponsoring some of the Drexel research because there is a fear terrorist could use E. coli to contaminate food.
Source: http://cbs3.com/health/local_story_319212219.html

[Return to top]

Water Sector

29. *November 14, KTRK News (TX)* — **Chemical waste being dumped into water treatment plant worries Pasadena, Texas, officials.** City of Pasadena, TX, officials are concerned about someone dumping chemical waste into the Vince Bayou Water Treatment Plant. The facility processes and treats water coming from residents' homes, but authorities believe a commercial truck is dumping waste water into the system through manholes at night. "When that type of

waste comes into our plant, it actually damages our plants by killing the good bacteria that help us with our waste water process," said engineering coordinator Sarah Metzgere. Public Works engineers say this dumping is not just illegal, but the chemical waste water will eventually create a public health threat. The city is asking residents to keep an eye out for commercial waste trucks seen in Pasadena at night.
Source: http://abclocal.go.com/ktrk/story?section=local&id=4762364

[Return to top]

Public Health Sector

30. *November 16, News (Australia)* — **Powerful strain of influenza strikes Australian nursing home.** A sixth person has died from a powerful strain of influenza that has struck the Jindalee Nursing Home in Canberra, Australia, confirmed Australian Capital Territory Health Minister Katy Gallagher on Thursday, November 16. Patients and staff at the nursing home on Thursday were offered anti−viral therapies, including the drug Tamiflu. Gallagher said that so far there had been 56 notified cases of the respiratory illness at Jindalee, including seven staff.
Source: http://www.news.com.au/story/0,23599,20769942−1702,00.html

31. *November 16, News−Medical (Australia)* — **Scientists find key to mutations in bird flu virus.** An international group of scientists say they have found two spots on the H5N1 bird flu virus that will need to mutate for the virus to infect people more easily. The scientists from Japan, Britain and the United States say the two specific spots on the genes of the virus appear to determine if it attaches more easily to bird or human receptors. It seems the virus has a surface protein called haemaggluttinin, that binds more easily to "receptors" lining respiratory tracts of birds, rather than receptors in humans, which effectively means that it easily causes disease in animals such as poultry, but is much harder for humans to be infected. However the experts fear the H5N1 virus, if it mutates to attach easily to human receptors, will infect more humans and trigger a pandemic which could kill millions of people. The discovery of the two spots will enable scientists to determine if any strain of H5N1 has the potential to cause a human pandemic.
Study: http://www.nature.com/nature/journal/v444/n7117/pdf/nature05 264.pdf
Source: http://www.news−medical.net/?id=21018

32. *November 16, Associated Press* — **Malaria drug's rebound in Malawi offers hope.** A crucial malaria drug that lost its punch in most countries because of germ resistance now appears to be highly effective again in one African nation −− a startling shift with implications for other tough bugs. It appears to be the first time a drug widely used against a killer disease has regained effectiveness after a break in use. The drug, chloroquine, was for many years the standard for treating malaria because it's very cheap, effective and safe. But in 1993, doctors stopped using it in Malawi because it was no longer effective in fighting most malaria cases. However, in recent years, researchers saw signs of genetic shifts in malaria that suggested it might again be vulnerable to chloroquine. University of Maryland researchers tested it in 105 malaria−infected children at a clinic in central Malawi. An astounding 99 percent of them were cured, far better than the results of two drugs tested on another group of children.
Study: http://content.nejm.org/cgi/reprint/355/19/1959.pdf?hits=20&
where=fulltext&andorexactfulltext=and&searchterm=christopher

+plowe&sortspec=Score%2Bdesc%2BPUBDATE_SORTDATE%2Bdesc&excludeflag=TWEEK_element&searchid=1&FIRSTINDEX=0&resourcetype=HW CIT
Source: http://www.chron.com/disp/story.mpl/world/4338362.html

33. *November 16, Associated Press* — **More than 700 sick on Atlantic cruise.** More than 700 passengers and crewmembers aboard a trans−Atlantic cruise have fallen ill with flu−like symptoms, cruise line officials said. The outbreak, believed to be norovirus, struck people aboard the Carnival Cruise Lines' Liberty, one of the world's largest cruise ships, according to a statement issued Wednesday, November 15, by the Miami−based company. The ship left Rome on November 3 with about 2,800 paying passengers and was due to arrive in Fort Lauderdale on Sunday. "Within 24 hours of sailing, they had a lot of people sick. It has tapered off considerably over the past couple days," said David Forney, with the Centers for Disease Control and Prevention in Atlanta.
Source: http://www.usatoday.com/news/nation/2006−11−16−cruise−sick_x .htm

34. *November 14, Scotsman (Scotland)* — **Technology to create deadly bacteria and viruses from scratch only years away from completion.** New technology that would give terrorists the power to create deadly bacteria and viruses from scratch is only years away from completion and threatens to make existing controls on biological weapons obsolete, experts warned Monday, November 13. Synthetic biology is an emerging field that allows scientists to build micro−organisms from simple genetic material, in theory enabling the creation of deadly pathogens such as ebola or anthrax without access to existing stockpiles of the bugs. The technology could also allow terrorists or scientists in rogue states to jumble the genetic signature of the bugs in order to render them unrecognizable to health experts dealing with an outbreak, potentially delaying treatment and preventing authorities from tracing the origin of an attack. The concerns were raised at a biosecurity conference at Edinburgh University Monday in the run−up to a major review of the Biological Weapons Convention in Geneva later this month. On the other hand, Alistair Hay, a toxicologist from Leeds University, said synthetic biology offered an opportunity to improve human health by, for example, allowing scientists to create DNA sequences that may help produce vaccines.
Source: http://thescotsman.scotsman.com/international.cfm?id=1681602 006

[Return to top]

Government Sector

35. *November 15, Press−Telegram (CA)* — **Suspicious package scare closes building.** The Los County Registrar−Recorder County Clerk's office was closed and one floor was quarantined Wednesday, November 15, after an envelope containing suspicious white powder and threatening language was discovered by an employee, officials said. Authorities received the call of a suspicious package about 11:30 a.m., PST, said Norwalk sheriff's Sgt. Craig Harman. Sheriff's deputies, the county fire department, county police, and the FBI all responded to the call. The powder was found with a letter that may have made threats to politicians and claimed the substance was the biological agent anthrax, he said. Though the FBI is not yet releasing what exactly the white power was, Harman said, no one was hospitalized in connection with the incident.
Source: http://www.presstelegram.com/news/ci_4668301

[Return to top]

Emergency Services Sector

36. *November 15, Daily News (CA)* — **System speeds 911 cell phone calls.** A new system that routes 911 calls from cell phone users in Los Angeles to the Los Angeles Police Department was completed Wednesday, November 15, with the promise of quicker emergency response times. Previously, calls were routed through the California Highway Patrol. At the urging of the Federal Communications Commission, the state has been enhancing wireless 911 technology and shifting responsibility for answering the calls to local agencies. The technology includes a mapping system that enables dispatchers to automatically determine the caller's location.
Source: http://www.dailynews.com/ci_4664500

[Return to top]

Information Technology and Telecommunications Sector

37. *November 16, eWeek* — **'Pump−and−Dump' spam surge linked to Russian bot herders.** The recent surge in e−mail spam hawking penny stocks is the handiwork of Russian hackers running a botnet powered by tens of thousands of hijacked computers. Internet security researchers and law enforcement authorities have traced the operation to a well−organized hacking gang controlling a 70,000−strong peer−to−peer botnet seeded with the SpamThru Trojan. According to Joe Stewart, senior security researcher at SecureWorks, the gang functions with a level of sophistication rarely seen in the hacking underworld. For starters, the Trojan comes with its own anti−virus scanner that removes competing malware files from the hijacked machine. Once a Windows machine is infected, it becomes a peer in a peer−to−peer botnet controlled by a central server. If the control server is disabled by botnet hunters, the spammer simply has to control a single peer to retain control of all the bots and send instructions on the location of a new control server. The bots are segmented into different server ports, determined by the variant of the Trojan installed, and further segmented into peer groups of no more than 512 bots. This allows the hackers to keep the overhead involved in exchanging information about other peers to a minimum, Stewart explained.
Source: http://www.eweek.com/article2/0,1895,2060235,00.asp

38. *November 15, IDG News Service* — **Pirated Vista may be useless, Microsoft says.** Microsoft said supposedly pirated copies of its new Vista computer operating system "will be of limited value" to those who use them. Microsoft responded Tuesday, November 14, to reports that some Websites have been circulating pirated copies of Vista and the Office 2007 applications suite. But Microsoft said in a prepared statement that those pirated copies of the OS won't work for long. "The copies available for download are not final code and users should avoid unauthorized copies which could be incomplete or tampered. This unauthorized download relies on the use of pre−RTM [release−to−manufacture] activation keys that will be blocked using Microsoft's Software Protection Platform. Consequently, these downloads will be of limited value," the statement said.
Source: http://www.infoworld.com/article/06/11/15/HNpiratedvistausel ess_1.html

39. *November 15, CNET News* — **Google, Yahoo, Microsoft adopt same Web index tool.** Search engine rivals Google, Yahoo and Microsoft are teaming up to make it easier for Website owners to make sure their sites get included in the Web indexes. The companies are adopting Google's Sitemaps protocol, available since June 2005, which enables Website owners to manually feed their pages to Google and to check whether their sites have been crawled. Website owners have had to follow similar processes at each of the other major search engines separately. Now Website owners will be able to go to one place for alerting all three major search engines to their Webpages, something they have been requesting for some time, said Tim Mayer, director of product management at Yahoo Search.
Source: http://news.com.com/Google,+Yahoo,+Microsoft+adopt+same+Web+index+tool/2100−1025_3−6136041.html

40. *November 15, Security Focus* — **Online attackers experimenting with embedding malicious code in video formats.** On Tuesday, November 14, anti−virus firm McAfee warned Windows users that the company had discovered a worm, dubbed W32/Realor, actively infecting Real Media files. The infected video files do not contain an exploit for the RealOne or Real players, but a hyperlink that points to a malicious Website. When infected files are opened, the victim is referred to the Website, which attempts to compromise their computer using a previously patched flaw in Internet Explorer. There are numerous disadvantages to using video files to carry malicious code, but using the technique may allow the attacker to take advantage of users' expectations, said Craig Schmugar, senior threat researcher with McAfee's anti−virus emergency response team. "A chunk of people generally regard video files as safe, where they might treat screensavers and Office documents with some caution," Schmugar said.
Source: http://www.securityfocus.com/news/11424

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 38809 (−−−), 4662 (eDonkey2000), 1027 (icq), 1028 (−−−), 38973 (−−−), 4672 (eMule), 25 (smtp), 10416 (−−−) 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

41. *November 15, KRDO (CO)* — **Bomb explodes inside Cinemark theater.** Colorado Springs police are looking for suspects who set off a bomb inside a crowded theater. The explosion went off at the Cinemark Theaters on Powers Boulevard shortly before 9 p.m. MST, Tuesday night, November 14. Investigators said it looked like a dry ice bomb that was contained inside a plastic bottle. The explosion did do some damage, but no one was hurt. Theater management

did evacuate the building and shut down the complex for the night.
Source: http://www.krdotv.com/story.cfm?nav=&storyID=1428

[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.