Department of Homeland Security Daily Open Source Infrastructure Report for 7 November 2008

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

- The Associated Press reports that an airline passenger was charged with resisting arrest and interfering with the operations of a flight crew aboard United Airlines Flight 645, from Puerto Rico to Chicago. The airline crew says the passenger became unruly, forcing the flight to land in North Carolina. (See item 7)
- According to eWeek, Newsweek reported that both the Democratic and Republican presidential campaigns had their IT systems hacked and infiltrated in recent months. Newsweek's sources speculated that the attacks were targeted attempts by foreign constituencies. (See item 21)

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 6, WCSC 5 Charleston* – (South Carolina) **18-wheeler flips, spills chemicals.** Nearly two days after a tanker flipped and spilled gasoline on I-526 in North Charleston, South Carolina, the North Charleston Fire Department and Coast Guard will be back on the scene to resume cleanup. An 18-wheeler flipped and spilled 8,000 gallons of gasoline and kerosene onto the Mark Clark Expressway at the westbound Virginia Avenue entrance late Tuesday night. Some of those chemicals spilled into a tidal marsh near the Cooper River, and the Coast Guard was called in to

search the area for any damage. Police have not released much information about the driver of the tanker, but say he has been charged with driving too fast for the conditions. No evacuations were made, and crews have been working to clean the site since Tuesday night. The westbound Virginia Avenue on-ramp entrance remains closed.
Source: http://www.live5news.com/Global/story.asp?S=9302886

2. *November 6, Associated Press* – (Georgia; North Carolina; Virginia) **Pipeline firm to pay fine for spills.** Federal officials say Plantation Pipe Line agreed to pay a $725,000 civil penalty for spills of jet fuel and gasoline in Virginia, Georgia, and North Carolina. The Alpharetta-based company also agreed to $1.3 million in new spill prevention safeguards to settle a lawsuit over alleged Clean Water Act violations. The lawsuit cited failure to have a spill prevention, control, and countermeasure plan for a 420,000-gallon oil storage tank at Newington, Virginia. Officials said Tuesday that on January 10, 2000, at least 100 barrels of jet fuel leaked from a pipeline in Newington, Virginia and some went into Accotink Creek. The following were also cited: spills affecting streams in Alexandria, Virginia, in 2002; Hull, Georgia in 2003; and Charlotte, North Carolina in 2006.
Source:
http://www.ajc.com/services/content/printedition/2008/11/06/pipelinespills.html

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *November 6, Mid-Hudson News* – (New York) **Entergy to spend $100 million for ISE upgrades at Indian Point.** Entergy will spend over $100 million to upgrade the Indian Point nuclear power plants in New York, based on recommendations from an independent safety evaluation (ISE) panel's report issued last summer. Corporate officials told a public meeting Wednesday night that while the ISE report said the plants are safe, some new initiatives should be considered. Entergy plans to accommodate the recommendations by providing new initiatives, including upgrading surveillance systems, updating communications, adding additional staff, and partnering with local high schools and colleges to train prospective workers. The estimated cost of the upgrade to the plant will be more than $100 million, and will take three to five years to complete. The panel looked primarily at issues like emergency preparedness, security, employee resources and retention, material condition, and public outreach. The panel did say that the nuclear power plant is safe, but that upgrades needed to be made in these areas to ensure safe operations.
Source: http://www.midhudsonnews.com/News/November08/06/IP_SIE-06Nov08.html

4. *November 6, Daily News of Newburyport* – (Massachusetts; New Hampshire) **Nuclear plant drill puts town to test emergency.** Local officials Thursday continued work on emergency plans in the event of a disaster at Seabrook Station nuclear power plant in New Hampshire. Local, state, and federal authorities gathered in the Emergency Management bunker beneath the Senior Center to practice what they would do if there was an emergency at the nuclear plant. In a drill evaluated by the Federal Emergency Management Agency, officials were briefed about a leak at the Seabrook Station and then proceeded doing the actions they would do normally in a time of emergency. "We had a scenario where it escalated into something bigger," the Amesbury, Massachusetts, mayor said. "First we had an alert, then pressure built and there was a release of radioactive steam. We have to find the wind direction, evacuate the kids and milk-producing animals." "In a real-life emergency, Seabrook would be giving updates to the Massachusetts Emergency Management Agency and then to Amesbury," the mayor said. The director of Amesbury's Emergency Management said additional information about the recent Seabrook siren drill would be forthcoming. The drill was the first since the sirens sounded last month.
Source: http://www.newburyportnews.com/punews/local_story_310221521.html

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

5. *November 5, Federal Reserve Bank of Dallas* – (Texas) **Dallas Fed establishes pilot bank advisory council.** The Federal Reserve Bank of Dallas today announced the establishment of a pilot Bank Advisory Council at its San Antonio Branch to enhance communication and feedback with area financial institutions. The pilot program will build upon outreach efforts by the Dallas Fed and its branches to area financial institutions. The Council — composed of nine bankers — is a pilot program aimed at providing Dallas Fed officials with grassroots information from area bankers on a variety of topics, including banking and economic conditions, regulatory issues, and Federal Reserve services. During its first year, the Council will meet quarterly and brief the San Antonio Branch board.
Source: http://dallasfed.org/news/releases/2008/nr081105.cfm
See also:http://www.mysanantonio.com/business/33939404.html

6. *November 5, WIRED News* – (New York) **Three plead guilty in $2 million Citibank ATM caper.** Three New Yorkers accused of using hacked Citibank ATM card numbers and PINs to steal $2 million from customer accounts in four months have pleaded guilty to federal conspiracy and access device fraud charges. The defendants are among 10 suspects charged earlier this year in connection with a breach of a server

that processes ATM transactions from 7-Eleven convenience stores. Those ATMs are branded Citibank, but they are owned by Houston-based Cardtronics. Court records indicate a Russian hacker cracked the ATM server in late 2007 and monitored transactions from 7-Eleven cash machines long enough to capture thousands of account numbers and PINs. The Russian then farmed out the stolen data to mules in the United States, who burned the account numbers onto blank mag-stripe cards and withdrew cash from Citibank ATMs in the New York area for at least five months, sending 70 percent of the take back to Russia.
Source: http://blog.wired.com/27bstroke6/2008/11/three-plead-gui.html

[Return to top]

Transportation Sector

7. *November 5, Associated Press* – (North Carolina) **FBI: Airline passenger restrained with duct tape.** An airline crew used duct tape to keep a passenger in her seat because they say she became unruly, fighting flight attendants and grabbing other passengers, forcing the flight to land in North Carolina. The woman, of Oswego, New York, is due in court Thursday, charged with resisting arrest and interfering with the operations of a flight crew aboard United Airlines Flight 645, from Puerto Rico to Chicago. She allegedly struck a flight attendant on the buttocks with the back of her hand during Saturday's flight, FBI sources said in a criminal complaint filed in U.S. District Court in Charlotte. She also stood and fell onto the head of a blind passenger and later started pulling the person's hair, the complaint stated. Ankle cuffs kept slipping off the woman, so the flight crew and two passengers were forced to use duct tape to keep her in her seat, the complaint states.
Source: http://ap.google.com/article/ALeqM5gANL2TjqHiZsNENPakkeFSNIsSYAD9493O003

[Return to top]

Postal and Shipping Sector

8. *November 5, Spokesman Review* – (Idaho) **Substance found in mail room was corn starch.** The powdery substance found in a North Idaho office mail room was mostly corn starch, according to the Kootenai County Sheriff's Department. Three people at a Louisiana Pacific Corporation office north of Hayden were in isolation after coming into contact with the powdery substance the morning of November 5, and about thirty other employees were kept in the building as hazardous-material crews investigated. "They determined that the substance was corn-starched based and was of no further hazard," according to a news release. The substance has been sent to a laboratory in Spokane for further testing. The investigation began about eleven a.m. when an employee at the Louisiana Pacific offices had experienced burning eyes after dumping a white powdery substance found in a postal service tray in the corporate mail room, officials said. According to the sheriff's department, two employees, who were nearby, complained of a similar burning sensation and were treated by medics and were in

isolation. Sheriff's department deputies sand Northern Lakes Fire Department crews responded. Investigators are working to track the source of the powder, which may have been in the mail room for several days, according to the sheriff's department.
Source: http://www.spokesmanreview.com/breaking/story.asp?ID=17601

9. *November 5, Courier Express* – (Pennsylvania) **Courthouse cleared after anthrax threat.** An Election Day anthrax scare was not taken lightly at the Jefferson County Courthouse November r 4. Crews from Jefferson County Emergency Management Agency, Brookville Fire Co., Brookville Borough Police Department and Clarion County Emergency Response Team treated this incident as if it was a "worse case scenario." While opening up the mail a woman from the Tax Claim Office found an envelope with a note inside that read "Can you spell Anthrax." The envelope had an out-of-state address. The evacuation took less than five minutes. No injuries were reported. Initial reports stated that there was no powder, but crews responded to the incident as if there was an actual danger. Crews from the Clarion County Emergency Response Team donned protective clothing and self-contained breathing apparatus and entered the courthouse, removing the letter and other possibly contaminated items in the Tax Claim office. Those items were bagged and sealed inside a plastic bucket and removed to the decontamination tent, where the outside of the bucket was hosed off. The sealed bucket was turned over to the Brookville Police to be held until the FBI could take custody. An inspector for the U.S. Postal Service was also on scene.
Source: http://www.leader-vindicator.com/site/news.cfm?newsid=20188904&BRD=2758&PAG=461&dept_id=572984&rfi=6

10. *November 5, Meadville Tribune* – (Pennsylvania) **Suspicious package at Cambridge Springs prison triggers bomb scare.** Three police agencies converged at the Cambridge Springs prison November 5 after a suspicious-looking package was x-rayed and appeared to contain a bomb. The superintendent said at 8:55 a.m. mail room employees reported that a package from incoming mail was examined after staff heard a beeping noise coming from the box. An X-ray revealed a device that appeared to be wrapped in wires, at which time the prison went into lockdown, the affected area was evacuated and all staff and inmates were accounted for. In addition to Cambridge Springs Police Department, personnel from the Pennsylvania State Police and the Erie Bomb Squad were called to the scene. After the contents of the package were verified as being a medical device and not a bomb, the prison resumed its normal operations at about 12:35 p.m.
Source: http://www.meadvilletribune.com/local/local_story_310225230.html

11. *November 4, Page News & Courier* – (Virginia) **Bomb scare at Stanley Post Office sparked by bag of 'suspicious' mail.** Deputies from the Page County Sheriff's Office responded to call about a "suspicious-looking" package at the Stanley Post Office on the morning of November 4. The call was later proved to be a false alarm. The post office was evacuated on the morning of November 4 after a plastic bag was found near the front door upon opening. Deputies received the call at around eight a.m. and were on the scene within the half hour. "We were able to confirm that there were no

explosives — just return mail in a plastic bag," said a deputy.
Source: http://www.rocktownweekly.com/pnc_details.php?AID=33037&CHID=42

[Return to top]

Agriculture and Food Sector

12. *November 6, Florida Times Union* – (Georgia) **USDA names 22 counties disaster areas.** The U.S. Department of Agriculture has declared 22 Georgia counties disaster areas as a result of damage from Tropical Storm Fay and eligible for assistance, the governor announced Wednesday. Based on USDA damage assessment reports, farmers in 22 counties experienced enough damage to peanuts, cotton and corn crops to qualify for the disaster declaration. That makes farmers in the counties eligible for low interest loans from their county Farm Service Agency.
Source: http://www.jacksonville.com/tu-online/stories/110608/geo_352581675.shtml

13. *November 5, Poultry Site* – (National) **USDA launches COOL listserv.** The U.S. Department of Agriculture's Agricultural Marketing Service (AMS) has launched a Country of Origin Labelling (COOL) listserv. The listserv will notify subscribers of significant additions to the all inclusive, information-packed COOL Web site. The COOL Web site offers detailed information for both industry and consumers. The Web site includes an assortment of resources, such as an extensive question and answer section, a Power Point presentation on the COOL Interim Final Rule and links to current and historical legislative information. Visitors also will find documents associated with the fish and shellfish rule, U.S. Customs and Border Protection rulings relative to COOL and more. The new COOL listserv will provide the benefit of reaching out to subscribers with immediate updates and help retailers to more easily achieve compliance with COOL requirements in a cost-effective manner.
Source: http://www.thepoultrysite.com/poultrynews/16357/usda-launches-cool-listserv

14. *November 5, United Press International* – (National) **Poultry industry may need genetic restock.** U.S. animal scientists say the poultry industry's commercial chickens are missing more than half the genetic diversity native to the species. A Purdue University Professor was part of an international research team that analyzed the genetic lines of commercial chickens used to produce meat and eggs around the world. The researchers found the birds' genetic deficits are possibly leaving them vulnerable to new diseases and raising questions about their long-term sustainability. "Just what is missing is hard to determine," the Purdue researcher said. "But recent concerns over avian flu point to the need to ensure that even rare traits, such as those associated with disease resistance, are not totally missing in commercial flocks." He said it's also important to preserve non-commercial breeds and wild birds for the purpose of safeguarding genetic diversity and that interbreeding additional species with commercial lines might help protect the industry.
Source:
http://www.upi.com/Science_News/2008/11/05/Poultry_industry_may_need_genetic_restock/UPI-11161225914564/

15. *November 5, Brownfield Network* – (Illinois) **EAB quarantine expands in Illinois.** The quarantine boundary for the Emerald Ash Borer has been expanded in Illinois to include parts of four more counties. The state agriculture department says two previously-unknown infestations of the destructive beetle have been confirmed in McLean County and previously infested areas. All of McClean and Woodford counties, along with eastern Marshall and parts of Livingston County that were not a part of previous orders, are included in the expanded quarantine area. That brings the total number of quarantined Illinois counties to 21. The movement of certain wood and nursery stock is prohibited from quarantined areas. Violators may be fined up to $500. The emerald ash borer, or EAB, has killed tens of millions of ash trees since it was discovered in the Midwest over six years ago. It's been detected in 10 states, so far, and Canada.
Source: http://www.brownfieldnetwork.com/gestalt/go.cfm?objectid=6EC6F411-5056-B82A-D04AEA99B2081988

[Return to top]

Water Sector

16. *November 5, WITN 7 Washington* – (North Carolina) **Massive sewage spill.** A privately owned wastewater treatment plant in Onslow County with a history of violations has failed again. The New River keeper in Jacksonville estimates for the past four to six months – 64-thousand gallons of raw sewage a day has been flowing out of the plant and into the ground. The plant is owned by Centerline Utilities. The spill was reported on October 31. The Division of Water Quality in Raleigh asked the Onslow Water and Sewer Authority to take over the plant and correct the problem. The New River keeper says this facility has several violations in permits over the years. The state is to make on site checks of these facilities every six months. It is unknown when the last inspection took place. Centerline Utilities has not been sending reports to the state about the plant for at least five-months. Centerline could face possible civil and criminal penalties.
Source: http://www.witn.com/home/headlines/33935534.html

17. *November 5, South Carolina Now* – (South Carolina) **Fallen tree leads to wastewater discharge into Jeffries Creek.** Florence city crews are cleaning and having water samples analyzed after a fallen tree caused an estimated 175,000 of wastewater to flow into Jeffries Creek, according to a city press release. The spill, reported around ten a.m. November 3, occurred near the Hampton Pointe subdivision in the Oakdale area. It was caused when the tree landed on an elevated sewer line on piers and cracked a manhole, according to the city. Crews removed the tree and stopped the discharge by 3:30 p.m. November 3, and they had repaired the manhole by noon November 4. The city reported the overflow as part of a South Carolina Department of Health and Environmental Control program to notify the public of wastewater discharges of 5,000 gallons or more.
Source:
http://www.scnow.com/scp/news/local/pee_dee/article/fallen_tree_leads_to_wastewater_discharge_into_jeffries_creek/18295/

[Return to top]

Public Health and Healthcare Sector

18. *November 6, Reuters* – (International) **Half of extensively drug-resistant TB patients die.** The hardest-to-treat form of tuberculosis kills half the people who get it, according to a South Korean study that is one of the few to track survival rates from the condition called extensively drug-resistant TB. Tuberculosis is an infectious bacterial disease typically attacking the lungs. Increasing numbers of cases of TB that defy standard medical treatment are appearing worldwide. The study tracked 1,407 patients with two categories of TB: multidrug resistant TB, or MDR-TB, which resists at least one of the two main TB drugs, and extensively drug-resistant TB, or XDR-TB, which defies nearly all drugs used to treat TB. Forty-nine percent of those with XDR-TB died compared to 19 percent of patients with ordinary MDR-TB, researchers at the Asan Medical Center in Seoul wrote on Thursday in the American Journal of Respiratory and Critical Care Medicine. TB killed 1.7 million people worldwide in 2006.
Source: http://abcnews.go.com/Health/Germs/wireStory?id=6194122

19. *November 6, Alexandria Town Talk* – (Louisiana) **Louisiana prepares for a pandemic flu outbreak; summit today.** Louisiana's health care experts and medical professionals discussed preparations for a pandemic flu outbreak Thursday at a pandemic flu summit at the Gillis Long Center in Carville. The Louisiana Department of Health and Hospitals and Office of Public Health, which hosted the event, taught the state's health care providers and emergency personnel about the virus and how to prepare their agency or facility for this threat. The state is also offering new training opportunities for health care professionals by offering a free Web-based pandemic flu course. The course will help provide doctors, nurses and allied health professionals the most up-to-date information on pan flu preparedness.
Source: http://www.thetowntalk.com/article/20081106/NEWS01/311060034

20. *November 5, U.S. Food and Drug Administration* – (National) **FDA reports nationwide recall of mislabeled ReliOn insulin syringes.** The U.S. Food and Drug Administration is notifying health care professionals and patients that Tyco Healthcare Group LP (Covidien) is recalling one lot of ReliOn sterile, single-use, disposable, hypodermic syringes with permanently affixed hypodermic needles due to possible mislabeling. The use of these syringes may lead to patients receiving an overdose of as much as 2.5 times the intended dose, which may lead to hypoglycemia, serious health consequences, and even death. The recall applies to Lot Number 813900, ReliOn 1cc, 31-gauge, 100 units for use with U-100 insulin. Only ReliOn syringes from this lot number and labeled as 100 units for use with U-100 insulin are the subject of the recall. These syringes are distributed by Can-Am Care Corp and sold only by Wal-Mart at Wal-Mart stores and Sam's Clubs under the ReliOn name.
Source: http://www.fda.gov/bbs/topics/NEWS/2008/NEW01911.html

[Return to top]

Government Facilities Sector

21. *November 5, eWeek* – (National) **Campaign hacks highlight cyber-espionage.** The security world is abuzz with news today that both the Democratic and Republican presidential campaigns had their IT systems hacked and infiltrated in recent months. As originally reported by Newsweek, "The computer systems of both the Obama and McCain campaigns were victims of a sophisticated cyber-attack by an unknown foreign entity, prompting a federal investigation." The newsmagazine also reported that after taking a closer look at the incidents, Obama's technical experts believed that the involved hackers were either Russian or Chinese. Newsweek's sources speculated that the attacks were targeted attempts by foreign constituencies to study the potential policies that each candidate would propose to put into place.
Source:
http://securitywatch.eweek.com/exploits_and_attacks/campaign_hacks_highlight_cyber-espionage.html

[Return to top]

Emergency Services Sector

22. *November 6, Washington Post* – (Virginia) **Federal funds support N.Va. hazmat teams.** Hazardous materials teams in Northern Virginia are receiving an infusion of federal money to bolster preparations for chemical, biological and other threats. The funds were on the way before dozens of threatening letters, some containing white powder, were sent last month to financial institutions and regulatory offices across the country. Test results have been negative for toxins, but the incidents have drawn renewed attention to such potential dangers and the ongoing needs of responders more than seven years after the Sept. 11, 2001, attacks on the World Trade Center and the Pentagon. The $190,000 in grants from the Department of Homeland Security has gone to hazmat teams in Arlington County and Alexandria, which have a combined squad, and Fairfax and Loudoun counties, state and local emergency officials said. Fairfax County Fire and Rescue, for example, has used its $30,000 grant to order a hazardous gas vapor identifier. Responders using the tool will be "better able to recognize hazmat situations quickly," said a spokesman for Fairfax County Fire and Rescue. The device also covers many other chemical agents. A spokesman for the Federal Emergency Management Agency, one of the federal sources of such funding, said the grants "can be used to prepare for, respond to and recover from acts of terrorism and natural disasters," including nuclear, chemical, radiological and explosive incidents.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/11/03/AR2008110303694.html

23. *November 5, Newsday* – (New York) **Mayday call probed as hoax.** A Mayday call to the U.S. Coast Guard about a sinking vessel in Oyster Bay Harbor is being considered the latest in a rash of hoax calls on Long Island that are currently under federal investigation, an official said. A Coast Guard spokeswoman said details regarding the specific number of hoax calls are not being released at this time, but she said numerous

incidents have occurred across the Island during the past month to two months. Coast Guard Station Eatons Neck, Nassau police and Suffolk police responded to the call but found no vessel and no missing boater. Reporting a false or fictional incident is a federal offense, a Coast Guard officer said. A felony, it is punishable by 6 years in federal prison and a $250,000 fine. "It's a waste of resources," she added. She said pursing hoax calls "puts our boat crews at risk" and could place boaters at risk — since crews could be pursuing hoax calls instead of handling real emergencies. She said the incidents are under investigation by Coast Guard investigators. Officials would not say whether any of the incidents are related.
Source: http://www.newsday.com/news/local/nassau/ny-lihoax1106,0,6136271.story

[Return to top]

Information Technology

24. *November 6, IDG News Service* – (International) **Once thought safe, WPA Wi-Fi encryption is cracked.** Security researchers say they have developed a way to partially crack the Wi-Fi Protected Access (WPA) encryption standard used to protect data on many wireless networks. The attack, described as the first practical attack on WPA, will be discussed at the PacSec conference in Tokyo next week. There, a researcher will show how he was able to crack WPA encryption and read data being sent from a router to a laptop computer. The attack could also be used to send bogus information to a client connected to the router. To do this, the researcher and his co-researcher found a way to break the Temporal Key Integrity Protocol (TKIP) key, used by WPA, in a relatively short amount of time: 12 to 15 minutes, according to the PacSec conference's organizer. They have not, however, managed to crack the encryption keys used to secure data that goes from the PC to the router in this particular attack
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9119258&taxonomyId=17&intsrc=kc_top

25. *November 6, Enterprise Security* – (International) **Fake site punts Trojanised WordPress.** Fraudsters have set up a fake site featuring a backdoored version of the WordPress blogging application as part of a sophisticated malware-based attack. The fake Wordpresz.org site offered up what purports to be version 2.6.4 of the open source blogging tool. In reality all but one of the files are identical to the latest pukka (2.6.3) version of WordPress. The crucial difference comes in the form of a Trojanised version of pluggable.php, according to a Sophos virus researcher. Sophos detects the malicious code as WPHack-A Trojan. The issue came to light via a posting by a blogger who reports that he received a "High Risk Vulnerability Warning" from the spoofed WordPress domain when he logged into his admin account. It looks like sites which have not upgraded to 2.6.3 are being exploited in an way where a hacker, probably using an automated script, hacks into sites with the vulnerability and changes the settings of one of the dashboard modules to point to a different feed, encouraging people to go to a different site which offers a dodgy upgrade. The fake site attack represents a rare but not unprecedented attack on users of the open source blogging package.

Source: http://www.theregister.co.uk/2008/11/06/trojanised_wordpress/

26. *November 5, Government Technology* – (National) **Malware campaign uses Obama's name.** The polls have been closed for less than 24 hours, and already hackers are launching a new malware campaign. Using the president-elect's name to draw people in, the e-mail messages contain subject lines such as "Obama win preferred in world poll" and claims to be from news@president.com. After the message is opened, there is a link that purports to take the user to news about the new president. Once the link is clicked, the user is prompted to download Adobe Flash 9 to view a video of Obama president making a speech. If the bogus Adobe Flash player is downloaded, a malicious Trojan horse infects the computer. SophosLabs identified this malware as Mal/Behav-027, and it has accounted recently for nearly 60 percent of malicious spam. Owners with infected computers will find that their data has been compromised, and they could potentially even have their identity stolen. Sophos experts said the malicious Trojan horse incorporates the following characteristics: The malware contains rootkit technology to conceal itself; it is designed to steal information from an infected computer; it has general "backdoor" functionality; it spies on user's keyboard and mouse inputs and can take screenshots; it looks for passwords; and it submits the information it discovers to a Web server located in Kiev, Ukraine. Users of anti-virus products should check to see if updates have been made to protect against this new malware.
Source: http://www.govtech.com/gt/articles/428384

Internet Alert Dashboard

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

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

27. *November 6, RCR Wireless* – (National) **Wireless providers protest backup-power reporting regs.** The cell phone and tower industries urged the current administration to reject backup power reporting requirements, arguing that the Federal Communications Commission grossly underestimated time, operational and financial burdens placed on wireless providers. Indeed, wireless providers argue information collection guidelines associated with the eight-hour cell site backup power mandate could trigger unintended consequences that are at odds the government's objective to maintain communications during and after major storms like Hurricane Katrina, which prompted FCC action. By FCC estimates it will cost each wireless carrier approximately $312,600 to adhere to backup power information collection requirements, the wireless industry predicts the financial hit would be exponentially greater. The administration could rule on the issue within days.
Source:

http://www.rcrwireless.com/article/20081106/WIRELESS/811059995/1099/wireless-providers-protest-backup-power-reporting-regs

28. *November 5, IDG News Service* – (National) **Clearwire still sees challenges after FCC OK.** The head of WiMax operator Clearwire said its work is just beginning after the U.S. Federal Communications Commission's (FCC) approval Tuesday of the company's joint venture with Sprint Nextel. The FCC voted on Tuesday to allow Clearwire and Sprint to form New Clearwire, a service provider that will combine the frequencies held by both entities and eventually build a national mobile broadband network. But the two carriers still only have one commercially available mobile WiMax network between them, in Baltimore, and the national infrastructure will have to be built from scratch in a harsh economic environment.
Source:
http://www.pcworld.com/businesscenter/article/153363/clearwire_still_sees_challenges_after_fcc_ok.html

[Return to top]

Commercial Facilities Sector

29. *November 6, Tonawanda News* – (New York) **Girl arrested for HS bomb threats.** Police in North Tonawanda arrested a 14-year-old girl as the sole suspect in a string of bomb threats called in to North Tonawanda High School recently. The girl, whose name was not released because she is a juvenile, is charged with four counts of falsely reporting an incident and will be arraigned in family court. Three threats in total were being investigated leading up to the arrest Wednesday afternoon, beginning with one Oct. 30, a second on Tuesday and Wednesday's incident. The latest messages were somewhat more specific than before, with one actually specifying to beware of 1 p.m. Wednesday. "We located the owner of the phone, her father brought her in, we spoke with her — she admitted to all four," the North Tonawanda Police Chief said.
Source: http://www.tonawanda-news.com/local/local_story_311000448.html

30. *November 4, WISC 3 Madison* – (Wisconsin) **Middleton teen arrested on suspicion of making bomb threat at high school.** A 16-year-old boy was arrested on suspicion of making the bomb threat at Middleton High School on Tuesday afternoon, which caused the students to be evacuated and forced election officials to move polling equipment. Authorities said that the incident began at about 3:03 p.m. and all the students were evacuated. Police said that the boy is a student at the high school. The teen was in the high school computer lab and accessed an Internet relay Web site. The Web site received the typed message from the student, then translated it into a verbal message and sent it to a high school official, according to authorities. Polling equipment at the high school was moved to the nearby fire station. Polling for Middleton aldermanic districts 5, 6, 7 and 8 were being held at the new Middleton Fire Department at 7600 University Avenue.
Source: http://www.channel3000.com/news/17895425/detail.html

[Return to top]

National Monuments & Icons Sector

31. *November 6, Stockton Record* – (California) **Bomb scare at Oak Grove closes Eight Mile Road.** An item thought to be an explosive device found at Oak Grove Regional Park forced the closure of Eight Mile Road for a time Wednesday morning. Stockton firefighters and an ambulance were called to the park as a precaution while bomb squad members dealt with the device. There was no immediate report if the item was an explosive device. The San Joaquin Metropolitan Bomb Squad responds countywide to any suspicious item that may be an explosive device. A Sheriff's deputy said details of the incident, including what the device was, whether it was explosive, and what was done with it, were not available Wednesday evening.
Source:
http://www.recordnet.com/apps/pbcs.dll/article?AID=/20081106/A_NEWS02/811060328/-1/A_NEWS07

[Return to top]

Dams Sector

32. *November 6, Associated Press* – (Washington) **Army Corps identifies leaking dam near Walla Walla.** A leaking dam near Walla Walla poses an "unacceptable" risk to the public and will be specially managed until it can be repaired, the U.S. Army Corps of Engineers said. The 67-year-old Mill Creek Storage Dam is seeping water and is especially dangerous when Bennington Lake is more than 17 percent full, the agency said November 5. It is typically kept just 5 percent to 10 percent full. The corps is in the process of evaluating all 610 of its dams nationwide for safety. Dams get a rating of one to five, with five being safest and one being the most at risk. The Mill Creek Dam is the only one in the Walla Walla District – which covers portions of Washington, Idaho, Oregon, Wyoming, Nevada and Utah – to be rated a one. The problems are that gravel and silt materials in the dam may be washing away, which promotes water seepage and could lead to collapse. The dam is also prone to earthquake damage. For now, the Corps will increase monitoring of the dam while seeking money to make improvements. The cost will not be known until any damage can be fully assessed. The Corps is also working with Walla Walla County to create an alert system and to place emergency supplies in advance of any problems.
Source:
http://ap.google.com/article/ALeqM5hlcD_PE2ZowhOwA11NmjhQXkP41QD949CSR80

[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 NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

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