Department of Homeland Security Daily Open Source Infrastructure Report for 24 October 2005

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

Daily Highlights

- The Atlanta Journal−Constitution reports state officials are notifying 465,000 Georgians that they might be at risk of identity theft because of a government security breach detected in April. (See item 6)
- Newsday reports a federal baggage screener at New York's John F. Kennedy International Airport stole $80,000 in cash from a checked suitcase belonging to a passenger bound for Pakistan. (See item 11)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *October 21, Department of Energy* — **Department of Energy seeks public comment on designation of western energy corridors.** The U.S. Department of Energy (DOE) announced that it and several other federal agencies will host eleven public meetings to discuss the designation of multi−purpose energy corridors on federal lands in the western United States. The recently passed Energy Policy Act of 2005 requires DOE, along with the Departments of Agriculture, Commerce, Defense and Interior, to identify possible corridors on federal lands in the west for new oil, natural gas and hydrogen pipelines and electricity transmission and distribution facilities.

Source: http://www.energy.gov/engine/content.do?PUBLIC_ID=19023&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE

2. *October 20, PRNewswire* — **New England could face electricity shortage in two years.** Experts say that New England's electric surplus could run out within 24 months, which could trigger rolling blackouts. An answer to the generation shortage could come in the form of Locational Installed Capacity (LICAP), in which suppliers are compensated for expanding their plants' generation capacity where extra electricity is most needed. According to Cindy Eid, executive director of the New England Coalition for Reliable Energy (NECORE), the implementation of LICAP "will make it easier and more affordable to start replacing aging, inefficient, and dirty plants with new, cleaner, and more efficient plants." LICAP is a concept proposed by the New England Independent System Operator (ISO−NE), a nonprofit corporation that coordinates the region's power supply and maintains the flow of electricity. Eid says, "Simply improving energy efficiency and conservation measures will not solve the problem alone. While such improvements would be desirable and indeed worthwhile, they won't be enough to satisfy future energy demand."
NECORE Website: http://www.necore.org
Source: http://www.prnewswire.com/cgi−bin/stories.pl?ACCT=104&STORY=/www/story/10−20−2005/0004173911&EDATE=

3. *October 13, Department of Energy* — **DOE releases roadmap for new biological research efforts.** The Department of Energy (DOE) has released a comprehensive plan, the GTL Roadmap, for a new generation of biology research that builds on genome project investments to help solve national energy challenges. Projects within the GTL Roadmap include utilizing microbial enzymes to improve the manufacture of ethanol from cellulose by replacing current processes that are inefficient and expensive. The proposed genomics GTL Roadmap was formulated over the last three years and is now being reviewed at the National Academy of Sciences. The final phase of the three−phase GTL research program utilizes knowledge to position GTL to rapidly transform new science into new processes and products to help meet critical national energy and environmental needs.
GTL Roadmap: http://www.sc.doe.gov
GTL program: http://www.doegenomestolife.org
Source: http://www.caprep.com/1005022.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *November 01, National Defense Magazine* — **Department of Commerce seeks data on industries affected by Katrina.** The Department of Commerce (DOC) has set up an Internet Web portal for the defense industry to report production or supply problems resulting from

hurricanes. Of particular concern is the damage caused to liquid hydrogen plants, which could affect defense suppliers in the space and munitions sectors. In the aftermath of Hurricane Katrina, DOC's Office of Strategic Industries and Economic Security (OSIES) was made responsible for identifying defense supply or production issues being experienced by industry, particularly by companies that are located along the Gulf Coast. OSIES has established a special e−mail address to receive reports from affected companies. Firms are asked to provide a written description of the specific damages and the impact on production and delivery. After Katrina hit, officials from DOC, DoD, and DHS concluded that the hurricane potentially would affect production of key materials used in military equipment. The area affected by Katrina is hosts 25 percent of the North American industrial base for liquid hydrogen production.
OSIES Website: http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/d efault.htm
E−mail address: Katrina.defenseindustry@bis.doc.gov
Source: http://www.nationaldefensemagazine.org/issues/2005/Nov/UF−Co mmerce.htm

5. *October 20, The Wall Street Journal* — **Contractors brace for potential Pentagon budget cuts.** Defense contractors may face one of the toughest Pentagon budget cycles in years. Pentagon officials say the administration is aiming to cut between $10 billion and $15 billion a year in planned defense spending from fiscal years 2007 to 2012, slowing the overall rate of Pentagon−spending growth. Given the continuing military operations in Iraq, the Pentagon is scouring weapons programs for possible cuts instead of taking reductions from current−force needs In November, the Office of Management and Budget will release budget guidance for the fiscal year beginning October 1, 2006, that will delineate which programs will receive budget cuts. Even with possible cuts, total Pentagon spending and procurement is still expected to rise in the coming five years, but at roughly half the growth rate of the previous five years.
Source: http://www.post−gazette.com/pg/05293/592030.stm

[Return to top]

Banking and Finance Sector

6. *October 22, Atlanta Journal−Constitution* — **Georgians at risk for identity theft.** State officials in Georgia on Friday, October 21, began notifying 465,000 Georgians that they might be at risk of identity theft because of a government security breach detected in April. Joyce Goldberg, spokesperson for the Georgia Technology Authority (GTA), said officials are alerting 244,000 motorists and 221,000 retired teachers, state employees, school employees and others who participated in the state Health Benefits Plan in 2002 that a former GTA employee downloaded their personal information to his home computers. Goldberg said that officials believe the breach occurred in 2002, though it wasn't detected until April. That's when another GTA employee questioned why programmer Asif Siddiqui was logged in after hours to a data system in which he was no longer supposed to be working. Siddiqui, a native of Pakistan who had worked at the GTA for four years, was fired April 29 and arrested on felony charges of computer trespassing and theft. Officials say they have yet to determine why Siddiqui wanted the information or why it appears not to have been used in three years.
Source: http://www.ajc.com/metro/content/metro/1005/21statecomputers .html

7. *October 21, Department of the Treasury* — **Treasury targets North Korean entities for supporting weapons of mass destruction proliferation.** The U.S. Department of the Treasury

on Friday, October 21, designated eight North Korean entities pursuant to Executive Order 13382, an authority aimed at freezing the assets of proliferators of weapons of mass destruction (WMD) and their delivery vehicles. The action prohibits all transactions between the designated entities and any U.S. person and freezes any assets the entities may have under U.S. jurisdiction. "Proliferators of WMD often rely on front companies to mask their illicit activities and cover their tracks," said Stuart Levey, the Treasury's Under Secretary for Terrorism and Financial Intelligence. "Today's action turns a spotlight on eight firms involved in WMD proliferation out of North Korea. We will continue to expose and designate these dangerous actors," said Levey. The designations are part of the ongoing interagency effort by the United States Government to combat WMD trafficking by blocking the property of entities and individuals that engage in proliferation activities and their support networks. The eight entities are Hesong Trading Corporation, Tosong Technology Trading Corporation, Korea Complex Equipment Import Corporation, Korea International Chemical Joint Venture Company, Korea Kwangsong Trading Corporation, Korea Pugang Trading Corporation, Korea Ryongwang Trading Corporation, and Korea Ryonha Machinery Joint Venture Corporation.
Source: http://www.treasury.gov/press/releases/js2984.htm

8. *October 20, Reuters* — **Court says U.S. can bar funds for terror groups.** The United States can designate foreign organizations as terrorist groups and bar Americans from financially backing them, a federal appeals court ruled on Thursday, October 20. "Leaving the determination of whether a group is a 'foreign terrorist organization' to the executive branch ... is both a reasonable and a constitutional way to make such determinations," Judge Andrew Kleinfeld wrote for a three−judge panel. The ruling by the 9th U.S. Circuit Court of Appeals was made in a case involving people who raised money in California for Mujahedin−e Khalq, or MEK, an Iranian opposition group designated as a terrorist organization by the U.S. government since 1997. The defendants argued the MEK was not a terrorist group and they had First Amendment rights to contribute to the group. The court disagreed, saying contributing money was not the same as exercising a right to free speech.
Source: http://www.alertnet.org/thenews/newsdesk/N20556227.htm

9. *October 20, Associated Press* — **Regulators order Deutsche Bank's U.S. operation to take steps to prevent money laundering.** The Federal Reserve (Fed) and state regulators have ordered the U.S. banking operation of Deutsche Bank, Germany's largest bank, to take steps to prevent money laundering after finding deficiencies in its controls. The Fed and the New York State Banking Department on Friday, October 21, announced an agreement with New York−based Deutsche Bank Trust Co. Americas, which was not fined under the accord. Under the agreement, the bank promised to tighten its policies and procedures, reporting of suspicious transactions and customer vetting to prevent money laundering. Deutsche Bank spokesperson Ted Meyer confirmed the bank's commitment to strengthen controls. “There have been no findings of money laundering, and the bank remains committed to a rigorous anti−money laundering compliance program,” he said in a statement.
Source: http://www.financetech.com/news/showArticle.jhtml?articleID= 172302743

[Return to top]

Transportation and Border Security Sector

10. *October 23, AFX (Nigeria)* — **No survivors in Nigerian plane crash.** None of the 117 passengers and crew on board a Nigerian airliner that crashed Saturday night, October 22, north of Lagos survived, the National Emergency Management Agency (NEMA) said. No one could have survived the impact when the Bellview Airlines Boeing 737 hit the ground at such speed that the wreckage was "completely buried under ground," said NEMA spokesperson Ibrahim Farinloye. The statement followed a similar report by the Nigerian Red Cross, which was working with NEMA on the ground at the crash site in Lissa village, a short distance north of Lagos near the farming town of Otta. The jet took off from Lagos airport shortly after nightfall on Saturday, during a powerful thunderstorm at the start of a scheduled flight to Abuja with 111 passengers and six crewmembers on board, according to the flight manifest.
Source: http://www.forbes.com/work/feeds/afx/2005/10/23/afx2293114.h tml

11. *October 22, Newsday (NY)* — **Screener caught in airport theft.** A federal baggage screener at New York's John F. Kennedy International Airport stole $80,000 in cash from a checked suitcase belonging to a passenger bound for Pakistan, officials said on Thursday, October 20. The passenger, 45, who owns a gift shop in Manhattan, checked the suitcase at Pakistani International Airlines Terminal 4 on October 7, prosecutors said. The man, who was not identified, handed it to a cousin, who took it to a secure screening area while the passenger said goodbye to his family, officials said. When the shop owner arrived in Karachi, the 800 $100 bills were missing. He called the authorities, and as part of the investigation, the cousin identified the screener with whom he had left the bags, prosecutors said. When confronted while on duty at the airport, the screener, Frank Ulerio Jr., 23, of Glendale, admitted stealing $60,000, and he had $18,000 of the money with him, officials said. Ulerio said he used part of the money to pay off a gambling debt, prosecutors said. "It is particularly troubling that an individual responsible for ensuring the safety and security of our nation's airlines and protecting us from terrorism would allegedly engage in such egregious conduct," Queens District Attorney Richard Brown wrote.
Source: http://www.newsday.com/news/printedition/newyork/nyc−nyair21 4478095oct21,0,5186711.story?coll=nyc−nynews−print

12. *October 22, Canadian Press* — **Canadian rail, transit operators seek government help.** Transport Minister Jean Lapierre plans to discuss with the cabinet soon ideas about increasing anti−terrorism measures aboard rail and mass transit systems, says a security adviser to his department. The Canadian federal government has put a special focus on drafting improvements to transit security following the bombings that rocked the London subway system during the summer. Margaret Purdy, a special adviser to the deputy minister of transport, said industry members are calling for more training, better emergency preparedness, additional anti−terrorism exercises and simulations, and better information sharing. Many also want more physical security measures in transit stations and aboard vehicles, including extra personnel and greater use of closed−circuit cameras, Purdy said Friday, October 21, after addressing the annual conference of the Canadian Association for Security and Intelligence Studies. Video technology, though not a panacea, can be useful in countering extremists, Purdy said, noting that recorded images of suspected bombers helped British police. Margaret Bloodworth, deputy minister of Public Safety, told the conference that Canadians might be willing to accept cameras in subway stations as a deterrent to a terrorist attack or other crime.
Source: http://www.canada.com/fortstjohn/story.html?id=3ed77379−a6a1 −4ad5−aee8−021c622d8cc0

13. *October 21, Associated Press* — **Airports to get $17 million in improvements.** The New York region's three major airports will get improvements totaling more than $17 million in the latest round of work authorized Thursday, October 20, by their operator, the Port Authority of New York and New Jersey. Money includes nine million to retain contractors for work at Newark Liberty International Airport; six million for runway repairs at LaGuardia Airport in New York; and $2.1 million to improve road safety and vehicle flow at 10 locations at John F. Kennedy International Airport in New York. The work will upgrade traffic signals and signs, realign roads, and install roadside barriers.
Source: http://www.usatoday.com/travel/news/2005−10−20−new−york−upgr ades_x.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *October 21, University of Wisconsin* — **Study shows deer in chronic wasting disease zone stick close to home.** Researchers studied the traveling behaviors of 173 radio−collared white−tailed deer in south central Wisconsin. The results, which surprised researchers by revealing how little deer move about the landscape, are important because they may help researchers and wildlife managers better understand how chronic wasting disease (CWD) spreads. "They are using small home ranges and not traveling long distances," says Nancy Mathews, a wildlife biologist at the University of Wisconsin. "The only dispersers are young males, and they only go five to seven miles before setting up a new home range." The results of the study are both encouraging and confounding, says Mathews. On the one hand, knowing more about how deer move about the landscape may help scientists home in on how CWD spreads among wild deer. On the other hand, the findings contradict the idea that deer are great travelers, moving long distances and possibly taking the disease with them. "Based on the behavior of these deer, we cannot account for the distribution of CWD on the landscape," says Mathews who, with her students, conducted intensive, year−round telemetric studies of deer fitted with radio transmitters for the past two−and−one−half years.
CWD Alliance: http://www.cwd−info.org/
Source: http://www.news.wisc.edu/11743.html

15. *October 21, Agence France Presse* — **Denmark to slaughter 41,000 hens after exotic Newcastle disease outbreak.** Denmark said it would slaughter 41,000 hens after veterinary authorities confirmed an outbreak of the highly contagious bird illness known as exotic Newcastle disease on a farm in the southwest of the country. The illness, also known as pneumoencephalitis, is a deadly viral infection but is harmless to humans. The farm, located near Broager, was placed under observation on Thursday, October 20, once the illness was suspected and laboratory tests on Friday, October 21, confirmed the outbreak. The farm has been quarantined and a six−mile security zone has been set up, reaching the German border, in

a bid to contain the disease.
Source: http://news.yahoo.com/s/afp/20051021/hl_afp/denmarkgermanypoultry_051021192318;_ylt=Atsx_VFMrHj1WT3mDaJVtUGJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Food Sector

16. *October 22, Food and Safety Inspection Service* — **Meat and poultry products recalled.** Ian's Natural Foods, a Revere, MA, firm, is voluntarily recalling approximately 11,200 pounds of ready−to−eat meat and poultry products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Saturday October 22. The products were produced on various dates between October 12 and 18 and were shipped to a Trader Joe's warehouse in Massachusetts for further retail distribution. The problem was discovered through company microbiological sampling. FSIS has received no reports of illnesses associated with consumption of the product. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_044_2005_relea se/index.asp

17. *October 20, Associated Press* — **Thailand lifts ban on U.S. beef.** Thailand is lifting their ban on U.S. beef, officials said Thursday, October 20. Thailand was among dozens of countries that banned U.S. beef in December 2003 following the discovery of a cow infected with mad cow disease in Washington state. Mad cow disease is medically known as bovine spongiform encephalopathy. In humans, the consumption of tainted meat has been linked to the deaths of more than 150 people, mostly in Britain, from a degenerative, fatal brain disorder known as variant Creutzfeldt−Jakob disease.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/10/20/AR2005102001792.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

18. *October 23, Agence France−Presse* — **Croatia kills thousands of birds to fight avian flu.** Croatian authorities continued to kill thousands of domesticated birds in an area where dead swans infected by bird flu were found. Veterinary teams were carrying out the cull, begun Saturday, October 22, in a two−mile radius around a lake in eastern Croatia where the swans were found. "All teams are on the spot and we expect to finish this work Monday, October 24, at the latest," said Mate Brstilo, head of the government's crisis panel monitoring the disease. It

is expected that more than 10,000 chickens and other poultry will be killed in the quarantined area around the eastern village of Zdenci. Croatia's agriculture ministry announced Friday, October 21, that samples from organs of six dead swans found at the Zdenci lake had tested positive for the H5 virus. However, it was not immediately possible to say whether the virus was the lethal H5N1 strain which has killed more than 60 people in Asia. The samples from the swans have been sent to a laboratory in Britain for further tests to determine the precise strain of the virus. Another five swans were found dead at a pond, also in eastern Croatia, and were sent to Zagreb for analysis.
Source: http://news.yahoo.com/s/afp/20051023/hl_afp/healthflucroatia_051023153157;_ylt=ArcFX2l0L62I_mpVVFkWFsGJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

19. *October 23, Associated Press* — **Asian bird flu spreads to England.** The British government said Sunday, October 23, that a strain of bird flu that killed a parrot in quarantine is the deadly H5N1 strain that has plagued Asia and recently spread to Europe. Scientists determined that the parrot, imported from South America, died of the strain of avian flu that has devastated poultry stocks and killed over 60 people in Asia the past two years, according to the Department for Environment, Food and Rural Affairs (DEFRA). Debby Reynolds, DEFRA's chief veterinarian, said the parrot was likely infected with the virus while it was housed in the country's quarantine system with birds from Taiwan. Tests conducted on the Taiwanese birds that had died were inconclusive, according to the department. DEFRA said the virus was most closely matched to a strain found in ducks in China earlier this year.
Source: http://apnews.myway.com/article/20051023/D8DE0KJ01.html

20. *October 22, MosNews (Russia)* — **New bird flu outbreak registered in Russia's south Urals.** A new outbreak of bird flu has been registered in the Chelyabinsk region, in Russia's South Urals. Thirty−three birds, among them turkeys, ducks, and chickens have died at two individual farms in the village of Sunaly, Troitsk district, head of the regional agricultulre department was quoted by Interfax news agency as saying on Saturday, October 22. "There are a total of 26 individual farms in the village. Tests have proven that the birds have died of bird flu." A quarantine has been imposed on the area. An Emergency Ministry official also said bird flu was suspected in a village in the Altai region, close to the Kazakh border, where 59 birds died in the village of Pokrovka on Saturday, October 22. Veterinary services said Friday, October 21, they suspected that the bird flu virus had now spread to 24 areas, of which 20 were in the Novosibirsk region of Siberia, three in the Kurgan region of Siberia, and one in the southern region of Stavropol, though tests were still ongoing.
Source: http://www.mosnews.com/news/2005/10/22/chelyabinskbirdflu.sh tml

21. *October 20, U.S. Centers for Disease Control Prevention* — **Pandemic influenza virus of 1918 declared a select agent.** The U.S. Centers for Disease Control and Prevention (CDC) published Thursday, October 20, in the Federal Register an interim rule declaring the strain of influenza responsible for the 1918 pandemic as a select agent. There are currently 41 other agents and toxins listed as select agents under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. This action follows recent work done by CDC scientists to successfully reconstruct the 1918 virus in hopes of better understanding it. The virus was reconstructed to aid public health officials in preparing for the possibility of another pandemic of influenza. It will also be helpful to biomedical scientists as they seek to understand

what made the virus so harmful and to develop better antiviral drugs and influenza vaccines. All entities that possess, use, or transfer the 1918 strain of influenza or the eight key gene regions of the 1918 virus are required to register with the CDC. People, labs, and other facilities that work with select agents are required to ensure that they can safely handle the virus. In addition, they are required to increase safeguards and security measures for the virus, including controlling access, screening personnel, and maintaining records to be included in a national database with records from others registered.
Source: http://www.cdc.gov/od/oc/media/pressrel/r051020.htm

22. *October 20, Yale University* — **Cell cultures can sort out Creutzfeldt−Jacob disease infectious agents.** Research in Japan and at Yale University School of Medicine shows that infection with a weak strain of Creutzfeldt−Jacob Disease (CJD) prevents infection by more virulent strains and that the protection requires persistent replication by the infectious agent, but not misfolded prions. These studies showed that a persistent protective CJD infection did not require cells from the immune system or misfolded prions. “We demonstrate a new and very sensitive assay for infection by these agents that can discriminate among different strains, such as those that cause sheep scrapie and human CJD,” said senior author Laura Manuelidis. According to Manuelidis protection with a weak animal agent may account for the low incidence of CJD linked to Mad Cow Disease in people. “Our plan is to use these rapid infectivity assays to identify the different agents −− including those linked to Mad Cow Disease −− on the molecular as well as biological levels,” said Manuelidis. “This, as well as our previous results showing that most of the abnormal prion protein can be separated from infectious particles, point to a virus as the causal agent.” said Manuelidis “These results are not consistent with the idea that abnormal forms of the prion protein are infectious.
CJD information: http://www.cdc.gov/ncidod/dvrd/cjd/index.htm
Source: http://www.yale.edu/opa/newsr/05−10−20−03.all.html

[Return to top]

Government Sector

23. *October 21, Government Technology* — **DHS receives $2.4 billion increase for 2006 appropriations.** The Department of Homeland Security (DHS) received increased funding and changes to its organization when President George W. Bush signed the FY 2006 Homeland Security Appropriations Act. In addition to certain organizational adjustments, the Department's FY 2006 Appropriations provides increased funding for 1,000 new Border Patrol Agents, greater explosive detection technology across transportation networks, and an integrated Preparedness Directorate to enhance coordination and deployment of preparedness assets and training.
Source: http://www.govtech.net/news/news.php?id=97029

24. *October 21, Associated Press* — **DHS sending liaison to New York.** The Department of Homeland Security (DHS) plans to improve communication and coordination with local officials during anti−terror operations by assigning a new liaison officer to New York's police headquarters in lower Manhattan. DHS is also considering sending a full time liaison to the Los Angeles Police Department, DHS spokesperson Russ Knocke said Thursday, October 20. In the future, homeland security officials will work to put out joint statements with local officials in

the event of a localized terror alert, Knocke said.
Source: http://www.cnn.com/2005/US/10/21/terror.agencies.ap/index.ht ml

[Return to top]

Emergency Services Sector

25. *October 19, Connection Newspapers (VA)* — **A host of new high tech tools in the works for Virginia county emergency responders.** As part of Fairfax County, VA's ongoing efforts to protect its citizens during large−scale disasters −− including both terrorist attacks and extreme weather −− a slew of new high−tech communication initiatives are being considered. The measures include the development of outdoor warning sirens in urban sections of the county, an AM radio station to broadcast emergency messages, a "Reverse 911" system −− allowing the county to call each home in a specific neighborhood or zip code −− and a regional wireless broadband network for first responders. Another initiative currently in the works is the creation of a "311 Call Center," which would allow residents to call an easy−to−remember emergency hotline during an incident. The county government already offers tools for emergency notification. One such method is the county's "Community Emergency Alert Network," which sends out e−mail, text messages, and cell phone calls in a crisis. The county can also broadcast emergency messages via Channel 16, the Internet, weather radio stations, and over a "crawl" on network television. The new strategies underway are intended to ensure that everyone is informed in a crisis −− including residents without access to the Internet, television, or radio.
Source: http://www.connectionnewspapers.com/article.asp?article=5748 4&paper=61&cat=109

[Return to top]

Information Technology and Telecommunications Sector

26. *October 21, Information Week* — **Major disruption in Level 3 network slows Internet traffic.** The Internet has been slower due to a major disruption of service from tier one carrier Level 3 Communications on October 21. The disruption caused increases in Internet response times and drops in availability. In addition, Websites were unreachable and service was shut off for some users. According to George Roettger, Internet security specialist for NetLink Services Inc, "I don't think I've ever seen an entire backbone network go down like that before."
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid= NXVYLVXLHSQCMQSNDBCCKHSCJUMEKJVN?articleID=172303270

27. *October 20, FrSIRT* — **HP OpenView operations and OpenView VantagePoint JRE vulnerability.** A vulnerability has been identified in HP OpenView Operations and OpenView VantagePoint. This could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an error in Java Runtime Environment (JRE) and may be exploited via a malicious Web page to read and/write arbitrary files on a vulnerable system and execute local applications with the privileges of the user running the untrusted applet.
Source: http://www.frsirt.com/english/advisories/2005/2150

28.

October 20, Federal Computer Week — **DOD, industry on alert for Wilma.** The Defense Department has put military and industry teams on alert to provide communications if Hurricane Wilma disrupts the operation of telephone and wireless networks in the country. According to Brig. Gen. Nick Justice, deputy program executive officer in the Army's Program Executive Office for Command, Control, Communications−Tactical (PEO−C3T), "Teams are standing up right now at Fort Monmouth, NJ." In addition, Army signal units, which operate the service's battlefield communications systems, are also on call. According to Brig. Gen. Carroll Pollett, commanding general of the Army's Network Enterprise Technology Command and 9th Army Signal Command located at Fort Huachuca, AZ. In addition, Industry officials with DataPath and Qualcomm said they have personnel and equipment ready to provide communications with the Army.
Source: http://fcw.com/article91167−10−20−05−Web

29. *October 19, Security Focus* — **Browser/Firefox crome page loading restriction bypass.** Mozilla Browser/Firefox are prone to a potential arbitrary code execution weakness. This may be used by an attacker to load privileged 'chrome' pages from an unprivileged 'about:' page. This issue does not pose a threat unless it is combined with a same−origin violation issue. This issue also may allow a remote attacker to execute arbitrary code and gain unauthorized remote access to a computer. This would occur in the context of the user running the browser.
Source: http://www.securityfocus.com/bid/14920/info

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports a vulnerability in the Snort Back Orifice Parsing Remote Code Execution the exploit is in Snort's Back Orifice pre−processor. A stack based overflow can be triggered with a single UDP packet, allowing an attacker to fully compromise a Snort or Sourcefire installation. X−Force believes this vulnerability to be trivially exploitable, and urges affected users to upgrade immediately. Snort is a widely deployed, open source network intrusion detection system (IDS). Snort and its components are used in other IDS products, notably Sourcefire Intrusion Sensors, and Snort is included with a number of operating system distributions.

Snort preprocessors are modular plugins that extend functionality by operating on packets before the detection engine is run. The Back Orifice preprocessor decodes packets to determine if they contain Back Orifice ping messages. The ping detection code does not adequately limit the amount of data that is read from the packet into a fixed length buffer, thus creating the potential for a buffer overflow. The vulnerable code will process any UDP packet that is not destined to or sourced from the default Back Orifice port (31337/udp). An attacker could exploit this vulnerability by sending a specially crafted UDP packet to a host or network monitored by Snort.

US−CERT is tracking this vulnerability as VU#175500 please review: http://www.kb.cert.org/vuls/id/175500

Top Source Port / IP Addresses: Increased reported port activity: 1026 UDP, 1026 UDP, 1029 UDP, 1030 UDP from the following IP blocks, located in China: 221.10.254.31,218. 66.104.208, 222.77.185.242, 221.27.16.180, 61.152.158.126, 221.6.77.72, 202.99.172.160, and 218.66.104.206

US−CERT strongly recommends that all users reference the Federal Emergency Management Agency (FEMA) Website for a list of legitimate charities to donate to their charity of choice. http://www.fema.gov/

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 135 (epmap), 139 (netbios−ssn), 4495 (−−−), 40000 (−−−), 25 (smtp), 2234 (directplay) 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

Nothing to report.
[Return to top]

General Sector

30. *October 24, Bloomberg* — **Hurricane Wilma speeds toward florida.** Hurricane Wilma accelerated toward southern Florida Sunday, October 23, where about 150,000 people fled inland ahead of the storm that was bringing winds of 115 mph and rain that could cause widespread flooding. Wilma, a Category 3 storm, was centered 120 miles west of Key West and headed northeast at 18 mph, based on an 11 p.m. advisory last night from the U.S. National Hurricane Center. Hurricane−force winds extend 85 miles from its eye. About 2,400 National Guard troops have been mobilized and an additional 3,000 are on call, Florida Governor Jeb Bush said Sunday. Key West International Airport, Marco Island Airport, Florida Keys Marathon Airport and the Key West Naval Air Facility were closed, Michael C. McCarron, a spokesperson for the San Francisco International Airport, said. Florida Power and Light Co. estimates service for as many as 2 million customers may be affected, the utility said Sunday in a statement. Port Tampa was closed and Port Everglades and Port Canaveral were scheduled to close yesterday.
Hurricane Wilma Public Advisory:
http://www.nhc.noaa.gov/text/refresh/MIATCPAT4+shtml/181440. shtml
Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=avYyJhb4 9mIk&refer=us

31. *October 21, Associated Press* — **Bomb threat disrupts traffic near Capitol.** A young man told police there was a bomb in his car in front of the Capitol on Friday, October 21, and police exploded a package inside the car as a precaution, authorities said. The man was taken to a Washington, DC hospital for a psychiatric evaluation, while another man in the car was questioned and released, said a federal law enforcement official. Work went on as usual inside the Capitol as police cordoned off several blocks nearby. Two young men in the car a gray 2005 Chevrolet Impala with Florida license plates were taken into custody, said U.S. Capitol Police spokesperson Jessica Gissubel.
Source: http://abcnews.go.com/Politics/wireStory?id=1237915

[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