Department of Homeland Security Daily Open Source Infrastructure Report for 17 November 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- USA TODAY reports the National Transportation Safety Board has ruled that existing airport runway safety systems are trouble−plagued, and close calls between jets are happening with alarming frequency. (See item 7)
- The Government Accountability Office has published a report entitled, Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security, which discusses the status of efforts to secure domestic air cargo. (See item 12)
- Newsday reports representatives from across the U.S. heard Israeli counterterrorism experts in Hauppauge, New York, in what was described as Long Island's first major conference on the topic. (See item 19)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

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

1. *November 16, Reuters* — **OPEC sees more oil demand in 2006.** The world will need the Organization of the Petroleum Exporting Countries' (OPEC) oil even more this winter and next year as high oil prices have failed to slow galloping economic growth, the producer group said on Wednesday, November 16. OPEC increased its world oil demand forecast for 2006 in its

monthly report, and also said demand for its own oil in the fourth quarter of this year would be 276,000 barrels per day (bpd) higher than previously expected. That is higher than cartel output of 30 million bpd. The cartel has raised its world demand growth forecast for 2006 to 1.52 million bpd. The increase of 0.05 million bpd over the previous month's estimate lifts 2006 demand to 84.8 million bpd. "These higher figures are supported by vigorous preliminary growth data from developing countries, a brighter outlook for the world economy −− particularly for the U.S. and Organization for Economic Cooperation and Development (OECD) Pacific countries −− and a rebound in Chinese apparent demand," according to the report.
OPEC November Monthly Oil Report:
http://www.opec.org/home/Monthly%20Oil%20Market%20Reports/20 05/pdf/MR112005.pdf
Source: http://www.nytimes.com/reuters/business/business−energy−opec .html

2. *November 16, Boston Business Journal* — **Grid operator repeats rolling blackout warning, urges options.** Grid operator ISO New England Inc. on Wednesday, November 16, formally reiterated comments in October to a Vermont newspaper that contracts held by power plants may not guarantee them adequate natural gas this winter, potentially triggering rolling blackouts during cold snaps. ISO New England is asking power plants to secure guaranteed fuel supplies, or be prepared to switch over to another fuel. ISO New England is also asking businesses to sign up for demand−reduction programs which give companies a break on their electricity rates in exchange for agreeing to curtail power use at peak demand, and for businesses and individuals to conserve energy.
Source: http://www.bizjournals.com/boston/stories/2005/11/14/daily32 .html?from_rss=1

3. *November 15, Associated Press* — **Improved results in tests of emergency sirens around nuclear plant.** Emergency sirens in the region around the Indian Point nuclear power plants showed some improvement in two tests Tuesday, November 15, with far fewer failures than in the two previous tests, the plants' owner said. The 156 rotating, pole−mounted sirens, dotted around the four counties within 10 miles of the plants, are meant to notify residents if there is an emergency at the plants that might affect them. On the first test, just two of the 156 sirens failed to sound, Entergy Nuclear Northeast spokesperson Jim Steets said. One failure was caused by a bad motor on the siren, Steets said, while the other was a communications failure, possibly interference with the radio signal that activates the sirens. That siren worked fine on the second test, but the one with the bad motor stayed quiet, as did four other sirens. Those all were due to the same sort of communication failure, Steets said, and "We believe that if we signaled them again, they would sound." Steets said Tuesday's improved results would not affect Entergy's pledge to replace the entire system with state−of−the−art equipment within two years. The Indian Point power plant is located in Buchanan, NY.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−ind ianpoint1115nov15,0,1983621.story?coll=ny−region−apnewyork

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *November 16, Online Chester (SC)* — **Chemical spill prompts evacuations in South Carolina.** A chemical spill at Omnova Solutions Inc. on the J.A. Cochran Bypass in Chester

County, SC, Tuesday morning, November 15, led to about 50 people being evacuated from their homes and businesses. At 9:34 a.m. EST a call was placed from Omnova to 911 regarding an unintentional release 20−400 gallons of a flammable substance called propionaldehyde. Chester Emergency Preparedness Director Eddie Murphy said that a strong wind that developed was a cause for concern. “With that wind blowing in the direction of the houses a decision was made to move the people out,” Murphy said. “Between 35 and 40 residents were evacuated, 10 people at the bus shop had to leave and about five people at Chad's Auto had to move out.” The area of evacuation covered about 300 meters. At about 10:30 a.m. evacuees were allowed to return to their homes and businesses.
Source: http://www.onlinechester.com/articles/2005/11/16/headlines/n ews3.txt

5. *November 15, News Tribune (WA)* — **Diesel fuel spills when bus, dump truck collide in Washington.** Two people were injured when a school bus and a dump truck collided Monday, November 14, in Midland, WA, a Central Pierce Fire and Rescue official said. The school bus was westbound on 112th Street−East when it struck the left side of the dump truck, said Assistant Fire Chief Matt Holm. The dump truck was headed southbound on Portland Avenue−East and making a left turn onto 112th Street, he said. The woman driving the bus and the man driving the truck both were taken to local hospitals, Holm said. There were no children on the bus. The crash forced officials to close the intersection for about an hour, he said. Traffic was diverted to Golden Given Road−East and Waller Road. The dump truck’s fuel tank was damaged in the accident and spilled about 50 to 60 gallons of diesel on the ground, according to Holm. Firefighters blocked nearby culverts and drains, and used foam to stop the fuel from draining away.
Source: http://www.thenewstribune.com/news/local/story/5333379p−4830 312c.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.

[Return to top]

Banking and Finance Sector

6. *November 16, Guardian Unlimited (UK)* — **UK watchdog warns of criminal gangs inside banks.** Britain's top financial regulator warned on Tuesday, November 15, of increasing evidence of sophisticated criminal gangs placing agents inside banks to carry out large−scale frauds. Callum McCarthy, chairman of the Financial Services Authority (FSA), said that scammers had been able to infiltrate financial services firms and get into a position where they could commit crime from within. "There is increasing evidence that organized criminal groups are placing their own people in financial services firms. They can increase their knowledge of firms' systems and controls and thus learn how to circumvent them to commit their frauds. There are links that need to be made here too between the work we do, the work firms do and the work of law enforcement," said McCarthy. Fraud within the financial industry costs the UK an estimated US$24 billion a year. McCarthy said there was a link between these crimes and terrorism −− claiming the banking industry could play a vital role in countering the threat from

extremists. "There is also the contribution that can be made to making terrorist activity more difficult by impeding or preventing the flow of illicit funds," said McCarthy.
Source: http://money.guardian.co.uk/news_/story/0,1456,1643860,00.ht ml

[Return to top]

Transportation and Border Security Sector

7. *November 16, USA TODAY* — **Runway near misses prompt urgent safety concern.** Close calls between jets happen with alarming frequency on the nation's runways and federal regulators need to find better ways to curb the problem, the National Transportation Safety Board (NTSB) ruled Tuesday, November 15. The NTSB said that existing runway safety systems are trouble−plagued and the government has been slow to make improvements. The findings were released as part of the agency's annual "Most Wanted" transportation safety enhancements for the U.S. aviation system. "This is a safety issue and needs to be fixed," said John Clark, chief of the NTSB aviation safety division. Despite numerous safety efforts, runway incidents have stubbornly refused to fall in recent years. In the fiscal year ending October 31, there were 324 runway incidents, according to the Federal Aviation Administration, which oversees aviation safety regulations. Most posed little risk of a crash, but as many as 30 serious near collisions occur each year. The NTSB highlighted several near collisions Tuesday. In each case, a flawed warning system put in place by the FAA did not prevent the incident.
Source: http://www.usatoday.com/travel/news/2005−11−15−runway−near−m isses_x.htm

8. *November 16, Seattle Times* — **Pilots mistake taxiway for runway at Sea−Tac.** At least eight times since December 1999, experienced pilots from five different airlines have mistaken Taxiway Tango for Runway 16R at Seattle−Tacoma Airport (Sea−Tac). Three planes, including an American Airlines MD−80 carrying 111 passengers and crewmembers, actually landed on the taxiway. Five others −− most recently in January of this year −− either performed last minute "sidesteps" to shift course and land on 16R, or aborted their landings before circling and touching down safely on the runway. The incidents have alarmed the highest levels of the National Transportation Safety Board (NTSB), which has repeatedly warned that the confusion could cause a collision between incoming jets and planes or vehicles on the taxiway. Among the steps Sea−Tac and the Federal Aviation Administration have taken to increase pilots' awareness about the Taxiway Tango situation is to add warnings to charts for the airport. No matter how Taxiway Tango is marked, electronic instruments can guide pilots precisely to Runway 16R. But on clear days pilots generally opt for visual approaches rather than relying on their instruments.
Source: http://archives.seattletimes.nwsource.com/cgi−bin/texis.cgi/ web/vortex/display?slug=seatac13&date=20051113&query=Sea+Tac +runway

9. *November 16, Department of Transportation* — **Additional $7.2 million to Mississippi airports damaged by Hurricane Katrina.** Three Mississippi airports will receive more than $7.2 million in federal funds to repair terminal buildings, hangars, airfield equipment and other facilities damaged by Hurricane Katrina, Department of Transportation Secretary Norman Y. Mineta said. The money will go to Gulfport−Biloxi International Airport, Stennis International Airport in Bay St. Louis, and Dean Griffin Memorial Airport in Wiggins. The funds come from

the Airport Improvement Program of the U.S. Department of Transportation’s Federal Aviation Administration. The latest grants bring the total value of hurricane relief from the Department to more than $12 million provided to Mississippi’s transportation system. The Department previously provided $4.5 million immediately following the disaster to airports in the Gulf region.
Source: http://www.dot.gov/affairs/dot16805.htm

10. *November 16, Reuters* — **Jet unlikely at fault in Air France Toronto crash.** The crash of an Air France jet in Toronto on August 2 does not appear to have been caused by problems with the Airbus A340 itself, Canada's Transport Safety Board said Wednesday, November 16. It described the events as follows: "After landing long, the aircraft overran the end of the runway and came to rest in a ravine just outside the airport perimeter." Some aviation analysts have said the ravine, about 650 feet beyond the end of the tarmac, should be filled in or covered to extend the runway's safety zone. All 309 people on board survived the crash in which the plane ran off the end of the runway as it landed during a severe thunderstorm. "To date, investigators have not found significant anomalies of the aircraft systems," the agency said in a preliminary report. "Review of digital flight data recorder data has not revealed any system troubles or malfunctions."
Source: http://www.usatoday.com/travel/news/2005−11−16−toronto−crash_x.htm

11. *November 15, Government Computer News* — **TSA releases guidance on biometrics for access control.** The Transportation Security Administration (TSA) has issued a guidance document on the basic criteria and standards the agency believes biometric technology should meet in order to qualify for airport access control systems. Congress mandated in the Intelligence Reform and Terrorism Prevention Act that TSA consult with representatives of the aviation and biometrics industries, as well as the National Institute of Standards and Technology, to develop the guidance package. The document is intended for two main audiences: airport operators, who own and operate the access control systems at their airports, and manufacturers of biometrics devices, whose products will be evaluated for inclusion on a Qualified Products List.
Biometrics guidance document: http://www.tsa.gov/interweb/assetlibrary/Biometrics_Guidance.pdf
Source: http://www.gcn.com/vol1_no1/daily−updates/37560−1.html

12. *October 17, Government Accountability Office* — **GAO−06−76: Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security (Report).** In 2004, an estimated 23 billion pounds of air cargo was transported within the United States, about a quarter of which was transported on passenger aircraft. Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) is responsible for ensuring the security of commercial aviation, including the transportation of cargo by air. To evaluate the status of TSA’s efforts to secure domestic air cargo, the Government Accountability Office (GAO) examined (1) the extent to which TSA used a risk management approach to guide decisions on securing air cargo, (2) the actions TSA has taken to ensure the security of air cargo and the factors that may limit their effectiveness, and (3) TSA’s plans for enhancing air cargo security and the challenges TSA and industry stakeholders face in implementing these plans. GAO recommends that DHS direct TSA to complete assessments of air cargo vulnerabilities and critical assets; reexamine the rationale for existing air cargo inspection exemptions;

develop measures to gauge air carrier and indirect air carrier compliance; assess the effectiveness of compliance enforcement actions; and ensure that the data to be used in identifying elevated risk cargo are complete, accurate, and current. DHS reviewed a draft of this report and generally concurred with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d0676high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−76

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *November 15, Associated Press* — **Washington University to study corn's genetic code.** Researchers at Washington University will lead a project to decipher the genetic code of corn, which they say should provide the knowledge leading to better corn yields. Corn is the second crop plant to have its genome sequenced. A team of scientists from 10 countries recently completed a similar project with rice. Washington University's Genome Sequencing Center received a $29.5 million grant from the National Science Foundation and the U.S. Department of Agriculture to decipher the genetic code of the most commonly used strain of corn, called B73. The U.S. Department of Energy, which has its own genome center, will use a $2.5 million grant to work simultaneously on a less common strain of corn, said lead investigator Richard Wilson. The corn genome is estimated to have 50,000 to 60,000 genes. Wilson said the research will help scientists better understand corn plants, and help breeders produce varieties with traits such as higher yield, improved nutritional content, and better resistance to disease, pests and drought. Actual sequencing begins December 1, with the first sequencing information to be made available to the public online starting in early 2006. Scientists estimate the project will take three years.
Source: http://www.oregonlive.com/newsflash/national/index.ssf?/base/national−4/11321027617510.xml&storylist=national

[Return to top]

Food Sector

14. *November 16, Agricultural Research Service* — **Natural substance reduces Campylobacter in chickens.** Proteins called bacteriocins, produced by bacteria, can reduce Campylobacter pathogens to very low levels in chicken intestines and could help reduce human exposure to food−borne pathogens, Agricultural Research Service scientists report. In a chicken's gut, the bacteriocins can crowd out pathogenic bacteria, making it less likely that pathogens could infect poultry or humans. Researchers evaluated tens of thousands of bacterial isolates from poultry production environments. The researchers have found promise in numerous organisms for anti−Campylobacter activity, namely Bacillus circulans and Paenibacillus polymyxa. In

addition, the researchers successfully enhanced the production of bacteriocins, making it much more attractive for industrial testing.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Water Sector

15. *November 15, New Mexican* — **Website offers drinking water information.** A new link on the New Mexico Environment Department has information on every public drinking water system in the state, from violations to number of customers. It contains contact information for local water system officials and the latest results from water tests that measure contaminants such as lead, mercury, and nitrates. Searches can be done by the name of the water system, town, county, or other data. It lists data for each drinking water system back to 1993 and is updated every two weeks.
Website: http://eidea.state.nm.us/SDWIS/
Source: http://www.freenewmexican.com/news/35047.html

[Return to top]

Public Health Sector

16. *November 16, Reuters* — **China confirms its first human cases of bird flu.** China confirmed on Wednesday, November 16, its first human cases of bird flu, adding to fears of a global pandemic in which millions of people could die. China's Ministry of Health reported two cases in the central province of Hunan and one in eastern Anhui, the official Xinhua news agency said. The World Health Organization (WHO) said one of the victims in Hunan was a girl of 12 who died last month. The WHO said it had been informed by China that a nine−year−old boy from Hunan province suspected of having bird flu was indeed stricken by the H5N1 virus, as was his 12−year−old sister. Chinese officials initially reported that the two children in Hunan had suffered pneumonia and not bird flu, but later invited international experts in to help investigate the cases. WHO spokesperson Roy Wadia said the third case was identified as a woman in Anhui province. "It's not a surprise. It shows that China like other countries that have bird flu in poultry can have human cases," Wadia said. Two additional suspected cases are a teacher in Hunan and a poultry worker in the northeastern province of Liaoning.
Source: http://abcnews.go.com/US/wireStory?id=1318120

17. *November 16, The News−Observer (Raleigh−Durham−Chapel Hill)* — **North Carolina surveillance system links hospitals.** On Wednesday, November 16, public health officials in North Carolina unveiled a powerful new tool for safeguarding public health: a statewide electronic surveillance system that will monitor hospital emergency room data for early signs of disease outbreaks and bioterrorism threats. North Carolina hospitals will submit information to the state every 12 hours about symptoms in patients seen at their facilities. If needed, the state could get data as often as every 15 minutes. State public health officials will have nearly real−time updates of emerging public health threats, which will allow the state to respond more quickly, contain disease outbreaks sooner, and save more lives, said Dr. Leah Devlin, the state

health director. "This is a constant electronic radar…If something blips on the screen, we see it and we go looking for it. This is not a passive system," she said. North Carolina officials think the new system is the first in the nation to electronically gather clinical and demographic information from emergency rooms statewide. Currently, 52 of the 113 hospitals in the state with 24−hour emergency rooms submit data to the North Carolina Hospital Emergency Surveillance System. By next spring, all of them will.
Source: http://www.newsobserver.com/104/story/367688.html

18. *November 16, Science and Development Network* — **South Asia to set up disease and disaster centers.** South Asian nations are to create two regional centers to detect and respond to natural disasters and emerging health threats such as bird flu. The seven−member South Asian Association for Regional Cooperation (SAARC) agreed on the plans in Dhaka, Bangladesh on November 12−14. India offered to host a regional disaster response center for disaster preparation and emergencies and the disease surveillance center will be set up in Bangladesh. The SAARC nations will also develop a regional strategy for facing infectious diseases such as bird flu, said Bangladesh's Prime Minister Khaleda Zia. Although South Asian countries have not yet reported any cases of bird flu, the past month saw new cases among both people and poultry in East and South−East Asia. The disease has killed 64 people in South−East Asia since 2003. All SAARC members −− Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan and Sri Lanka −− have banned poultry imports from affected countries. The SAARC leaders said that authorities in each nation should share information and experiences in disaster detection and emergency relief with each other.
Source: http://www.scidev.net/news/index.cfm?fuseaction=readnews&itemid=2480&language=1

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

19. *November 15, Newsday (NY)* — **Counterterrorism conference held in New York.** Some 400 Suffolk and Nassau, NY, law enforcement members, and representatives from across the U.S. came to hear Israeli counterterrorism experts in Hauppauge, NY, Monday, November 14, in what was described as Long Island's first major conference on the topic. Suffolk District Attorney Thomas Spota echoed the widely held view that another terror attack in the United States is likely, and said Long Island needs to become better prepared to deal with terror threats. Faced with a sprawling suburban landscape, law enforcement officials said they were focused on "prevention." Suffolk Police Commissioner Richard Dormer said police officers already receive daily e−mail bulletins about terrorist attacks, including incidents in far−off places, such as the recent bombings in Jordan. "This all comes down to the officer on the street, and him being alert and noticing something that's out of place," Dormer said. However, local officials seemed not yet prepared to ramp up security −− such as random bag searches

employed by the city police department in the subways in recent months.
Source: http://www.newsday.com/news/local/longisland/ny−literr1116,0,202549.story?coll=ny−linews−headlines

20. *November 15, Government Computer News* — **Technology, training go hand in hand in improving police communications.** About 60 percent of Department of Homeland Security grants to state and local governments in the last four years have been for interoperable communications, according to James Turk, program manager for the Office of Domestic Preparedness. However, officials are discovering that buying hardware is only a first step. "Training is suddenly raising its head as a real problem," Turk said Tuesday, November 15, at a discussion sponsored by the Industry Advisory Council. Police equipped with new digital voice and data systems often revert to older, more familiar channels during crises, according to Turk. Montgomery County, MD, is eight years into a program to provide high−bandwidth mobile data services to its 1,600 officers. The program has taken twice as long and cost twice as much as expected. Technology is only a tool, according to David Lynn, director of the Montgomery County police technology division, adding that to be useful, it requires training, cultural change and technical support. Additionally, he has found that firefighters adapt to the same technology more quickly than police since they are routinely testing it in situations outside the norm. As a result, when crises occur, firefighters are less likely to revert to old habits of communication.
Source: http://www.gcn.com/vol1_no1/daily−updates/37559−1.html

21. *November 15, North County Times (CA)* — **California terrorism drill ends, reveals minor communication gaps.** A full−scale terrorism exercise held Tuesday, November 15, in California, dubbed the "Golden Guardian," was a stressful day for many of the 1,200 participating law enforcement officers, firefighters, medical personnel, dispatchers, and volunteers. "Remember, the goal of an exercise is not for everything to work perfectly," said Deborah Stoffen, director of the San Diego County's Office of Emergency Services. The purpose, Steffen said, was to develop the capabilities of the departments, agencies and personnel, and to find areas in need of improvement. As the day ended, San Diego County Sheriff's Department Captain Glenn Revell said the agencies had learned the need for accurate communication under the stress and pressure of an event that didn't stop. "We didn't see any glaring areas that required improvement," he said. Many things went well, including partnering with area hospitals and paramedics, hazardous materials response planning, and an overall effort to handle terrorism, said Revell. However, two immediate lessons learned were the need for better security and better communications between the hospital and the disaster site, said Steve Miller, the Scripps Memorial Hospital's director of emergency services. A full formal assessment of the exercise will be issued in the upcoming weeks.
Source: http://www.nctimes.com/articles/2005/11/16/news/top_stories/ 111505182838.txt

[Return to top]

Information Technology and Telecommunications Sector

22. *November 15, Government Technology* — **Federal Communications Commission Launches VoIP 911 Website.** The Joint Federal Communications Commission (FCC) and National Association of Regulatory Utility Commissioners (NARUC) Task Force on VoIP 911 Enforcement has launched a new Website to provide consumers, industry, and state and local

governments information about the rules that require certain providers of Voice over Internet Protocol (VoIP) services to supply 911 emergency calling capabilities to their customers. FCC Chairman Kevin J. Martin said, "Anyone who dials 911 has a reasonable expectation that he or she will be connected to an emergency operator; this expectation exists whether that person is dialing 911 from a traditional wireline phone, a wireless phone, or a VoIP phone. This new Website will provide an easy way for consumers, industry, and other government agencies to get the most current information on this important issue."
FCC/NARUC Task Force website: http://www.voip911.gov.
Source: http://www.govtech.net/news/news.php?id=97263

23. *November 15, Techweb* — **IM worms mutating at an alarming rate.** Instant−messaging (IM) threats are mutating at an alarming rate, as virus writers attempt to bypass security−system updates that corporations use for protection. A record number of IM threat mutations have been recorded by IMlogic Inc., which has found that 88 percent of all worms tracked by its threat center also have mutations. The worst chameleon is the Kelvir worm, which has mutated 123 times during the last 11 months, the Waltham, Mass., vendor said. Art Gilliland, vice president of product for IMlogic, said, "IM threats are different than email threats. Updating virus signatures doesn't work well for IM, because the mutations are exceedingly fast and so is the speed with which these threats propagate."
Source: http://www.techweb.com/wire/security/173603062

24. *November 15, FrSIRT* — **Macromedia Flash Communication Server denial of service vulnerability.** A vulnerability has been identified in Flash Communication Server MX, which could be exploited by attackers to cause a denial of service. This flaw is due to an unspecified error when processing malformed Routing Table Maintenance Protocol data, which could be exploited by attackers to cause server instability or crashes. This vulnerability is triggered by a single alpha release build of Flash Player 8.5 (build 133). FrSIRT reports that Macromedia has released a fix.
Fix: http://www.macromedia.com/support/flashmediaserver/downloads_updaters.html
Source: http://www.frsirt.com/english/advisories/2005/2441

25. *November 15, FrSIRT* — **Macromedia Contribute Publishing Server password encryption issue.** A vulnerability has been identified in Macromedia Contribute Publishing Server, which could be exploited by attackers to gain knowledge of sensitive information. This flaw is due to a design error where a weak password encryption mechanism is used to create the shared connection keys, which could be exploited to disclose sensitive information (e.g. FTP login credentials). The vulnerability affects Macromedia Contribute Publishing Server (CPS) version 1.1 and prior. FrSIRT reports that Macromedia has released an upgrade.
Upgrade: http://www.macromedia.com/support/cps/downloads.html
Source: http://www.frsirt.com/english/advisories/2005/2440

26. *November 15, FrSIRT* — **Apple iTunes "CreateProcess" local privilege escalation vulnerability.** A vulnerability has been identified in Apple iTunes, which could be exploited to obtain elevated privileges. This flaw is due to an error in the way iTunes launches its helper application and searches system paths using the "CreateProcess()" and "CreateProcessAsUser()" functions to determine the program to run, which could be exploited by a local user to create an environment where a malicious program will be executed with the

privileges of the user running the vulnerable application. The affected product is Apple iTunes 5 for Windows XP/2000. FrSIRT reports that Apple recommends an upgrade to iTunes 6.
Upgrade: http://www.apple.com/itunes/download/
Source: http://www.frsirt.com/english/advisories/2005/2443

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 is aware of a buffer overflow vulnerability in Macromedia Flash Player versions 7.0.19.0 and earlier. If exploited, the vulnerability could allow a remote attacker to execute arbitrary code with privileges of the user on the affected system. We are not aware of any public exploits at this time. For more information about this vulnerability please see review the following URL's:

Vulnerability Note VU#146284:
http://www.kb.cert.org/vuls/id/146284

MPSB05−07 Flash Player 7 Improper Memory Access Vulnerability:
http://www.macromedia.com/devnet/security/security_zone/mpsb 05−07.html

Users who have already upgraded to Flash Player 8 are not affected by this issue.

US−CERT encourages users to upgrade to the appropriate software version as described in the Macromedia Security Bulletin at URL:
http://www.macromedia.com/resources/security/

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 80 (www), 25 (smtp), 27015 (halflife), 1434 (ms−sql−m), 139 (netbios−ssn), 135 (epmap), 53 (domain) 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

27. *November 16, Government Accountability Office* — **GAO−06−251T: Capitol Visitor Center: Update on Schedule and Cost (Testimony).** The Government Accountability Office (GAO) is

pleased to assist the Subcommittee in monitoring progress on the Capitol Visitor Center (CVC) project. GAO's remarks will focus on (1) the status of the project schedule since the Subcommittee’s October 18, 2005, hearing on the project, (2) the project’s costs and funding, and (3) worker safety issues. GAO will discuss the progress made and problems encountered in completing scheduled construction work and in continuing to develop the project schedule, as we indicated during the Subcommittee’s October 18 hearing. To help ensure that Congress receives a more reliable estimate of the project’s completion date in order to plan for the CVC’s opening to the public and make more informed decisions about funding needs for CVC construction and operations, GAO recommends that the Architect of the Capitol (1) implement the recommendations (which are consistent with prior recommendations on schedule management) made by its construction management contractor in its November 9 report on its schedule evaluation; and (2) reassess its proposal to open the CVC in mid−December 2006 when it is confident that it has a project schedule that reflects realistic durations, enhanced logic, the resolution of concerns expressed by the Fire Marshal Division, and the impact of delays and contract changes.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−251T

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

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

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

Department of Homeland Security Disclaimer

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.