



Department of Homeland Security Daily Open Source Infrastructure Report for 11 January 2007

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- TechWeb reports three technology companies have developed a communications system for miners and say they have made the first wireless phone call from a thousand feet inside a coal mine; this should greatly improve safety by giving miners a way to communicate with the outside world during a disaster. (See item [2](#))
- The National Transportation Safety Board, after reviewing the October 2004 crash of a small plane in Missouri, said the accident shows a need for regional air carriers to adopt more stringent professional standards for pilots -- as major airlines have done -- and improve training procedures for pilots flying at high altitudes. (See item [14](#))

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. *January 10, Platts Energy Bulletin* — **U.S. Coast Guard sets security zone around Georgia LNG terminal.** The U.S. Coast Guard has issued an interim rule establishing a permanent security zone around El Paso Corp.'s Elba Island, GA, liquefied natural gas (LNG) terminal, saying the addition of two berths for LNG tankers had increased security risks associated with the facility, documents show. The service said that in an expansion completed in early 2006, the terminal operator "inadvertently" created a "safe refuge off the Savannah River with

unrestricted access to LNG berths. As a result, the LNG facility and arriving LNG vessels are put at risk of sabotage or other adverse action that could result in significant damage to property and a loss of life." The service said its concern was "confirmed" in June 2006 when a sailing vessel entered the LNG slip and anchored for six hours, one day before the scheduled arrival of an LNG tanker. The Coast Guard said the incident prompted the terminal operator to conduct a visual inspection of above-water mooring features and complete an underwater survey to ensure the berth was safe for the tanker.

Source: <http://www.platts.com/Natural%20Gas/News/6338085.xml?sub=Natural%20Gas&p=Natural%20Gas/News>

2. *January 10, TechWeb* — **First wireless phone call made from inside coal mine.** Three technology companies that have developed a communications system for miners say they have made the first wireless phone call from a thousand feet inside a coal mine. Hannah Engineering, Rajant, and Sanmina-SCI say the jointly developed system was tested in mid-December in a former mine near Pittsburgh, PA, that's now used for research and testing by the National Institute of Occupational Safety and Health. "This is the first time a phone call has ever been made from inside a mine," says Peter Lenard, senior Vice President for Rajant. "We're on the cutting edge." Wireless communication from within a mine is expected to greatly improve safety by giving miners a way to communicate with the outside world during a disaster. The system, which is undergoing more tests and is expected to be commercially available in the second quarter, would provide voice communications, as well as the ability to track the whereabouts of each miner.

Source: <http://www.informationweek.com/showArticle.jhtml;jsessionid=QDTZNGTKAATOKQSNDLRSKH0CJUNN2JVN?articleID=196802591>

3. *January 09, Associated Press* — **Bush lifts Alaska oil, gas drilling ban.** President Bush lifted a ban Tuesday, January 9, on oil and gas drilling in Alaska's Bristol Bay, an area known for its endangered whales and the world's largest run of sockeye salmon. The action clears the way for the Interior Department to open 5.6 million acres of the fish-rich waters northwest of the Alaska Peninsula as part of its next five-year leasing plan. "There will be significant opportunities for study and public comment before any oil and gas development could take place," said Interior Secretary Dirk Kempthorne. But he said the bay, as well as expanded drilling in the Gulf of Mexico, "will enhance America's energy security." There are believed to be 200 million barrels of oil and five trillion cubic feet of natural gas beneath the bay's federal waters three miles to 200 miles from shore. The Interior Department last year estimated energy development could produce up to 11,500 jobs and new tax revenue for the state. Kempthorne also announced the department would raise the royalty rate for new deep-water oil and gas leases in the Gulf of Mexico to 16.7 percent.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/09/AR2007010900824.html>

4. *January 09, Reuters* — **Trans Alaska oil pipeline restarts after shutdown.** The Trans Alaska Pipeline System (TAPS) was restarting Tuesday afternoon, January 9, after a shutdown of about six hours caused by a leak, said its operator, Alyeska Pipeline Service Co. The oil spill was detected nearly 200 miles south of the giant Prudhoe Bay field on Alaska's North Slope, said Alyeska and Alaskan state regulators. The pipeline system carries about 800,000 barrels of crude per day. Up to 500 gallons of crude oil were spilled before the line was shut down,

Alaska environmental regulators said. The spill has since been contained and is being cleaned up. Alyeska is still investigating what went wrong, said Alyeska spokesperson Mike Heatwole. "What we really want to find out is why (a threaded fitting) was loose in the first place," he said. Earlier Tuesday, the on-scene coordinator for the Alaska Department of Environmental Conservation, Ed Meggert, said the cause of the leak was likely a faulty weld.

Source: http://today.reuters.com/news/articleinvesting.aspx?type=bon dsNews&storyID=2007-01-10T010022Z_01_N09184065_RTRIDST_0_ALA SKA-PIPELINE-LEAK-UPDATE-3.XML

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[[Return to top](#)]

Defense Industrial Base Sector

Nothing to report.

[[Return to top](#)]

Banking and Finance Sector

5. *January 10, Washington Post* — **U.S. bars Iranian bank to curb access to dollars.** The Bush administration Tuesday, January 9, barred Iran's oldest bank from doing any future business in the U.S., accusing the financial institution of transferring Iranian missile payments to North Korea. The move will prevent Bank Sepah, Iran's fifth-largest bank, from conducting business in U.S. dollars and is part of a larger White House plan, put in place last year, to cut off Iran's access to U.S. and European currencies. Though U.S. officials say the effort is aimed at the Tehran government, it is also likely to affect millions of Iranian citizens who conduct personal business in U.S. dollars and who travel overseas. Bank Sepah has nearly 300 branches in Tehran plus offices in Paris, Frankfurt and Rome as well as a British subsidiary, Bank Sepah International. U.S. law has long prohibited Iranian government institutions from doing business in the U.S., but yesterday's move now bars Sepah from converting international transactions into dollars by routing them through New York banks.

Department of the Treasury press release: <http://www.treasury.gov/press/releases/hp219.htm>

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/09/AR2007010901466.html>

6. *January 09, Finextra (UK)* — **Bank of America and Wells Fargo offer \$80,000 for arrest of ATM thieves.** Bank of America and Wells Fargo are offering a reward of \$40,000 each for information leading to the arrest and conviction of thieves who stole ATM units in the greater Maricopa County area of Arizona. The incidents occurred in the late night and early morning hours of February 19, July 27, September 8, and October 2 and 18 of last year. Each case involved the use of stolen heavy-duty construction equipment to remove or rob the ATM machines.

Source: <http://finextra.com/fullstory.asp?id=16349>

7. *January 09, IT Week (UK)* — **Personal details are being revealed online.** The results of a survey of PC users show that 45 percent of what we do online requires us to disclose personal or financial data. The survey, by Kaspersky Lab, shows that despite the increase in backdoor Trojans, keyloggers, and internet scams such as targeted phishing attacks, Web users have not been put off going online to conduct their banking, shopping, and travel bookings. "We are now so at ease giving out our personal data online that there is a risk of becoming complacent and falling for a phishing scam. These scams are getting more and more sophisticated and in some cases, harder to spot," said David Emm of Kaspersky Lab.

Source: <http://www.itweek.co.uk/computing/news/2172165/personal-details-revealed>

8. *January 09, BizReport* — **Phishers using Flash instead of HTML.** In an attempt to circumvent browser phishing detectors, phishers have begun to use Flash instead of HTML. The existing anti-phishing devices scan a Web page's HTML code to detect whether it is a fraudulent attempt to dupe users. Because Flash files are seen by these detectors as a single object they aren't scanned and the site user will not be warned of a potential risk. The technique is similar to how spammers started using images in e-mails in the hope that it would outsmart any filters. More often than not, these phishing sites are fake login pages, Web forms or password reset pages that require the user to input personal data such as a password, credit card number or social security number.

Source: http://www.bizreport.com/2007/01/phishers_get_flash.html

9. *January 09, InternetNews* — **Retiree data lost in laptop theft.** Following a theft of several laptop computers from a benefit consultant, retirees are being urged to monitor credit records. The five laptops stolen last month contain personal information of Towers Perrin clients' current and retired employees, said the pension and 401K management giant. In a statement, the company said it recently became aware of the theft of five laptops. Towers Perrin offered few details, except that the lost data includes "personal information" about clients "current, and possibly, former employees." The number of people affected by the data breach is unknown. The company said it was still compiling a list of employees impacted by the incident. Because the investigation was continuing, a company spokesperson wouldn't comment on when the laptops were stolen. Reportedly, a former employee was arrested December 28 by New York police. Towers Perrin said it is reviewing its security measures. All company laptops are password-protected, according to the spokesperson. Potentially, personal data available to benefit planners includes names, addresses, Social Security numbers and account information. Towers Perrin, however, said it had "no knowledge that any of this has been misused."

Source: <http://www.internetnews.com/security/article.php/3652901>

[\[Return to top\]](#)

Transportation and Border Security Sector

10. *January 10, Boston Globe* — **Switch eyed in Massachusetts rail deaths.** An improperly set track switch sent a commuter train barreling into a repair crew on Tuesday, January 9, killing two workers and injuring four others, two critically. After hitting the track maintenance vehicle

just before 2 p.m. EST, the Lowell-to-Boston train screeched to a halt, tossing the 43 passengers in their seats, slightly injuring 10 who were treated at Winchester Hospital. Officials identified the workers who were killed as Christopher Macaulay, 30, of Brentwood, NH, and James Zipps, 54, of Lowell, MA. Massachusetts Bay Transit Authority (MBTA) officials said they were investigating why the track switch did not shift the No. 322 train onto the parallel outbound tracks and instead sent it straight into the six-member crew, one operating the maintenance vehicle, the others working nearby. The track switches are remotely set from an operations center in Somerville, which controls train movements north of Boston. MBTA Transit Police and the National Transportation Safety Board plan to focus on the mechanics of the switch itself and the actions of the Somerville dispatcher, officials said. The dispatcher, who was responsible for setting the switch and monitoring the track, has been placed on paid leave during the investigation, said Scott Farmelant, spokesperson for the commuter rail system.
Source: http://www.boston.com/news/local/articles/2007/01/10/switch_eyed_in_rail_deaths/

11. *January 10, Boston Globe* — **MBTA to receive security grant.** Federal homeland security officials have announced that the Massachusetts Bay Transit Authority (MBTA) will receive \$15 million to bolster security on trains and buses, the largest single security grant it has ever received, as part of an effort to beef up "high-risk and high-consequence areas" underground and underwater. In addition, the Port of Boston was elevated to a higher-risk category by the Department of Homeland Security, making it eligible to seek a larger share of federal funding when maritime security grants are awarded later this year. Officials stressed, however, that the new ranking did not indicate any new threat. MBTA plans to use its new funding to increase security around rail and bus yards, enhance video surveillance at stations, and expand a pilot program for a system used to detect biological, nuclear, radiological, and explosive material in the subway system, officials said. The grant will also allow the MBTA to improve security on buses, which could include adding surveillance cameras.
Source: http://www.boston.com/news/local/articles/2007/01/10/t_to_receive_15_million_security_grant/

12. *January 10, USA TODAY* — **US Airways increases offer for Delta.** US Airways moved on Wednesday, January 10, to break the logjam in its offer to buy bankrupt Delta Airlines, upping its bid to \$10.2 billion, a 20 percent increase over the airline's \$8.5 billion proposal issued last November. The enhanced offer is designed to bypass Delta's management, which opposes the merger idea, and to appeal directly to Delta's creditors. Everyone from Delta's financial lenders, bondholders and Boeing, has been divided over whether US Airways' initial offer was a better deal than Delta management's alternative plan to emerge from Chapter 11 later this year as an independent carrier Delta's management has said its stand-alone plan would value the carrier at between \$9.5 billion and \$12 billion. Delta issued a statement on Wednesday saying that its board will review the revised US Airways offer. But it added that the higher bid "on its face... does not address significant concerns" raised about the initial US Airways proposal. One of those concerns was the high debt that the "new" Delta would be saddled with, a load that would grow another \$1 billion under the revised US Airways offer.
Source: http://www.usatoday.com/travel/news/2007-01-10-us-airways-increases-offer-to-merge-delta_x.htm

13. *January 10, Seattle Times* — **Seattle-Tacoma radar prompts warnings.** After repeated safety warnings from air-traffic controllers, Federal Aviation Administration (FAA) officials said

Tuesday, January 9, they will upgrade software to combat "ghost" radar images that can confuse the people guiding airplanes to and from Seattle–Tacoma (Sea–Tac) International Airport. Controllers complain that recurring "false targets" on the radar system sometimes force them to redirect planes to avoid what looks like an impending collision with one of these ghost aircraft. In one of many reports filed with the FAA since November, National Air Traffic Controllers Association union representative Dan Olsen wrote that the malfunctions were "extremely dangerous and stressful on the controllers. ... Fix the radar before someone is killed." Several experienced controllers said that while Olsen's language may be alarmist, the radar concerns he is raising are valid and many false targets show up daily. The FAA, while acknowledging the need for improved software that's scheduled to be installed at month's end, denies there's a safety issue. The radar system in question, at the Terminal Radar Approach Control (TRACON) facility, controls planes within a 40–mile radius of Sea–Tac. The TRACON facility is beside the third runway under construction at Sea–Tac and is fed data by a 200–foot–tall square radar tower nearby.

Source: http://www.king5.com/business/stories/NW_011007WABTIMESairtrafficontrolJM.27aad35a.html

14. *January 10, Pine Bluff Commercial (AR)* — **Pilots blamed in commuter jet crash.** Two pilots who took their commuter jet on a high–altitude joyride, then failed to follow proper procedures after both engines failed, were to blame for the October 2004 crash of the plane in Jefferson City, MO, federal investigators said Tuesday, January 9. But the National Transportation Safety Board (NTSB) said the accident shows a need for regional air carriers to adopt more stringent professional standards for pilots — as major airlines have done — and improve training procedures for pilots flying at high altitudes. While Memphis–based Pinnacle had pilot safety procedures in place in 2004, the NTSB said the program was not as rigorous as that of Northwest Airlines, its parent company at the time of the accident. Pinnacle has since adopted a more rigorous safety program. The safety agency also found the plane's engines had a history of locking up at high altitudes during test flights and that flight manuals did not explain the importance of keeping a minimum air speed to keep engine cores rotating. The NTSB called the "core lock" issue a contributing factor in the crash and recommended that the Federal Aviation Administration require aircraft manufacturers to perform tests on planes equipped with General Electric Co.–made CF34–1 or CF34–3 engines.

Source: <http://www.pbcommercial.com/articles/2007/01/10/ap-state-ar/d8mibbd00.txt>

15. *January 09, WLBT3 (MS)* — **Chemical found in passenger's baggage.** There was a scare at Mississippi's Jackson–Evers International Airport Tuesday, January 9, when screeners found a chemical in some baggage. Emergency crews were called in to investigate. A passenger apparently needed the chemicals for his job and put them inside his checked baggage. Officials say a passenger told them the substance was "water treatment chemicals." Sources said the chemicals were ammonia and bleach which becomes hydrochloric acid when combined. Three Transportation Security Administration employees were taken to the hospital as a precautionary measure after complaining of breathing problems. No flights were affected and no charges are expected to be filed against the passenger.

Source: <http://www.wlbt.com/Global/story.asp?S=5915935&nav=2CSf>

[[Return to top](#)]

Postal and Shipping Sector

16. *January 10, U.S. Postal Service* — **USPS: Intelligent Mail to be operational by 2009.** The U.S. Postal Service (USPS) on Wednesday, January 10, presented its new vision to revolutionize business mail by using standardized intelligent barcodes, continuous mail tracking, and real-time feedback to business customers. These services, referred to as Intelligent Mail, will be fully operational for all commercial mailers by 2009. “Intelligent Mail is like having a GPS system for mail,” said Postmaster General and Chief Executive Officer John E. Potter during the January Board of Governors meeting where the vision was presented. The centerpiece of the technology is one standardized intelligent barcode used on each piece of mail (letters and large envelopes known as “flats”) as well as each mail container. As these travel through the postal network, and are scanned at key points, the technology enables business customers to “see” their mail at every step — from arrival at the postal facility to processing to transportation to delivery. The Intelligent Mail process is fully automated. This sophisticated system enables real-time data to be captured and communicated — identifying problems such as bad addresses and improper pre-sort and feeding the information back to the mailers for correction.

Source: http://www.usps.com/communications/news/press/2007/pr07_002.htm

[\[Return to top\]](#)

Agriculture Sector

Nothing to report.

[\[Return to top\]](#)

Food Sector

Nothing to report.

[\[Return to top\]](#)

Water Sector

17. *January 10, WLUC6 (MI)* — **Iron Mountain adding chlorine to water system.** The city of Iron Mountain, MI, is putting chlorine in the water system to get rid of bacteria. The city's water last month tested positive for coliform — a naturally occurring bacteria that indicates the presence of contamination in water supplies. This is the second time in a year that the city has found coliform in the water. The state environmental department is requiring Iron Mountain to continue putting chlorine in its system until this spring.

Source: <http://www.wlns.com/Global/story.asp?S=5914265&nav=0RbQ>

18. *January 09, WorldWatch* — **China's rural residents see hope for safe drinking water.**

Nearly 312 million rural Chinese residents have no access to safe drinking water, facing problems of shortage as well as severe contamination. These rural populations suffer frequent and serious health attacks as a result of drinking unsafe water. The threats come from both

naturally occurring contaminants such as arsenic, fluorine, and salt as well organic and industrial pollution caused by human activities. To address this challenge, the central government has promised in its latest Five Year Plan (2006–10) to make safe drinking water available to 160 million rural residents by 2010, giving priority to areas that face contamination from fluorine, arsenic, salt, pollution, and the schistosoma worm, which can attack people's blood and liver and lead to schistosomiasis, or snail fever. The government has also set an ambitious target of providing all of China's rural residents with clean drinking water by 2015. This is the same year the United Nations hopes to reach its goal of reducing by half the number of people worldwide without sustainable access to safe drinking water.

Source: <http://www.worldwatch.org/node/4827>

[\[Return to top\]](#)

Public Health Sector

19. *January 10, RIA Novosti (Russia)* — Mysterious disease kills Indonesians. Twenty people died of a mysterious infectious disease in Indonesia in the last few months of 2006, a health official said Wednesday, January 10. I. Nyoman Kandun, head of the ministry's communicable diseases control center, told RIA Novosti that all the victims were patients at St. Carolus Hospital, in the Indonesian capital, Jakarta. The latest case was registered November 27. The newly discovered disease is characterized by a high fever, which usually leads to the patient's death within three days of its onset. Blood samples of those affected have been sent for tests to the U.S. Centers for Disease Control and Prevention.

Source: http://www.postchronicle.com/news/breakingnews/article_21258_237.shtml

20. *January 10, Bloomberg* — Rift Valley fever may be spreading in Horn of Africa. A Rift Valley fever outbreak that killed at least 75 people in Kenya the past month may be spreading in the Horn of Africa, aided by floodwaters harboring mosquitoes that carry the viral disease. Seven people may have died from the disease in an area of southern Somalia 11 miles north of the Kenyan border, where conflict between Islamist fighters and a transitional Somali government is hampering efforts to investigate suspected cases. "The dead are mainly nomadic herders," Hassan Mursal, a medical officer at the nearby Afmadow hospital said. "The number could be higher but, because of the current insecurity in the area, there is no way of getting the full picture." At least 235 cattle, camels, sheep and goats have died from Rift Valley fever in Kenya's Northeastern province, Bernard Omwoyo Moenga, assistant director of the country's Veterinary Research Laboratories said. A further 4,000 animals were infected and 27,000 were susceptible to infection.

Rift Valley fever information: <http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/rvf.htm>

Source: <http://www.bloomberg.com/apps/news?pid=20601085&sid=aXAA0px3xBfw&refer=europe>

21. *January 10, Agence France–Presse* — Indonesian teenager dies of bird flu. An Indonesian teenager died of bird flu, bringing the country's death toll from the disease to 58, a hospital official said. She said that the 14-year-old boy from Serpong, southwest of Jakarta, was one of two confirmed cases of bird flu treated at the hospital. Five other patients were suspected of being infected with the bird flu virus but there had not yet been any laboratory confirmation, she added. The boy was admitted to the hospital on January 5 and doctors have said some

chickens had died in his neighborhood a few days earlier.

Source: http://news.yahoo.com/s/afp/20070110/hl_afp/healthfluindonesia_070110055408

22. *January 10, Reuters* — China reports first human bird flu case in months. A 37-year-old farmer in eastern China has been confirmed to have contracted the H5N1 strain of bird flu, the country's first human case of avian influenza in months, the Health News said on Wednesday, January 10. The country has reported a total of 22 human cases of bird flu, including 14 fatalities, since 2003. In the latest case, a man developed symptoms of fever and pneumonia on December 10 and was discharged from hospital on Saturday, January 6, in Tunxi in Anhui province after a full recovery. China last reported a human case of bird flu in July, when a farmer died of H5N1 in the northwestern region in Xinjiang.

Source: <http://www.alertnet.org/thenews/newsdesk/PEK168523.htm>

23. *January 10, McClatchy Newspapers* — Whooping cough making a comeback. Despite widespread vaccination for whooping cough — about 86 percent of children nationally receive the immunizations to protect against the disease, according to the National Center for Health Statistics — the old foe is on the rise. During the 1930s and '40s, whooping cough sickened an average of 200,000 people a year and killed about 4,000 annually. After immunizations were introduced in the 1940s, the number of whooping cough cases nationally fell to a low of about 1,000 a year in 1976. But the U.S. Centers for Disease Control and Prevention has observed a 25-fold increase in reported cases of the disease since then. Whooping cough is the only vaccine-preventable disease that is increasing in the U.S. Medical experts think the increase is a result of waning immunity in adolescents and adults, whose childhood shots for whooping cough essentially wear off over time. Waning immunity would be no cause for concern if whooping cough weren't still circulating in the community, said Jeffrey Engel, North Carolina's state epidemiologist. He said outbreaks can often be traced to groups or individuals that haven't been immunized for medical or religious reasons. Last year, more than 25,000 cases of whooping cough were reported nationally.

Whooping cough information: <http://www.cdc.gov/doc.do/id/0900f3ec80228696>

Source: <http://www.recordonline.com/apps/pbcs.dll/article?AID=/20070110/LIFE/701100330>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

24. *January 10, Federal Computer Week* — Report: States, localities to invest more in communications technology. State and local governments will boost their technology investment by 40 percent in the next five years as they struggle to overcome communications problems that stymie coordinated emergency response efforts, according to a report released January 10. Technology spending will rise from \$3.2 billion in 2006 to \$4.4 billion in 2011 as public safety agencies push to bring real-time and on-demand communications to response

efforts, according to market analyst firm Datamonitor. But despite increased spending, those initiatives could run into a raft of problems, according to the report, including limited funding for new purchases, insufficient coordination among independent organizations, and confusion over which technology approach to adopt.

Report available for purchase:

<http://www.datamonitor.com/~a2faa4b8c9954b89a4d78bc321765aa7~/industries/research/?pid=DMTC1674&type=Report>

Source: <http://fcw.com/article97309-01-10-07-Web>

25. *January 09, WRAL-TV (NC)* — North Carolina first responders to get high-tech help.

Wake County, NC, has a plan to modernize the way emergency units are dispatched. County officials are trying to improve response times with a Global Positioning Satellite (GPS) system in the vehicles of first responders. The tracking units are already installed in all crime scene investigation vehicles. The county's ambulances will soon get GPS technology, and sheriff's cars will follow. "We hope it'll shorten our response time and always make sure that the closest ambulance is dispatched to the emergency," said Wake County EMS Chief Skip Kirkwood. Officials said GPS is the only way to get an exact location for every unit.

Source: <http://www.wral.com/news/local/story/1130931/>

26. *January 09, Daily Astorian (OR)* — Tsunami warning system gets in gear. The city of Seaside, OR, is working on new tsunami warning sirens, an automated phone system to call locals with emergency updates and instructions, a tsunami education coordinator and outreach program, evacuation caches with emergency supplies, and subsidies for household weather radios. The new sirens will have a bigger range and broadcast messages, such as whether the siren is a test. The emergency phone system could warn the public of tsunamis, fire evacuations, chemical spills, or other emergencies. The 911 dispatchers will activate it to call all buildings within the affected area with a recorded message explaining what is happening and what action to take. City Planner Kevin Cupples wants the system to call cell phones, too. It is hoped this will limit 911 calls from people who want information.

Source: <http://www.dailyastorian.com/main.asp?SectionID=2&SubSectionID=398&ArticleID=39373&TM=76364.4>

[[Return to top](#)]

Information Technology and Telecommunications Sector

27. *January 10, IDG News Service* — U.S. commerce secretary says China is thwarting global technology innovation by not embracing 3G standards. Secretary of the U.S. Department of Commerce Carlos M. Gutierrez Tuesday, January 9, criticized China for delaying the creation of a 3G (third generation) wireless network in that country, saying it is thwarting global technology innovation by not embracing standards. Speaking in a session at the International Consumer Electronics Show (CES) in Las Vegas, NV, Gutierrez said companies around the world must support common standards to promote a worldwide environment for technology innovation, not have their own "pockets of standards." He used China, where the government continues to hold out on granting licenses to build 3G networks, as an example of that misstep. China has delayed plans to build a 3G network for several years, he said. Many believe it is because the government wants to promote its own homegrown 3G standard, called

TD-SCDMA (Time Division Synchronous Code Division Multiple Access), instead of embracing a version of CDMA (Code Division Multiple Access), on which other countries have built or are building 3G networks. To do its part to encourage competition in the technology industry, the U.S. has to revise current legislation that governs the technology industry and remain as hands-off as possible, he said.

Source: http://www.infoworld.com/article/07/01/10/HNusslapschinafor3G_1.html

28. *January 10, Network World* — **Adobe releases first set of patches for cross-site scripting vulnerability.** Adobe late Tuesday, January 9, released the first set of security patches to address the cross-site scripting vulnerability disclosed by European researchers late last year. The flaw allows Acrobat Reader v.7.0.8 and earlier versions to be exploited by hackers. Left unpatched, the vulnerable versions of Adobe's Reader, Acrobat Standard, Acrobat Professional and Acrobat 3D let an attacker easily include JavaScript code in a browser session so that when a user clicks on a malicious link to a PDF on the Web, the attack code is activated. There is no vulnerability associated with PDF itself. The latest version of Acrobat, v.8, released in December, isn't vulnerable to the cross-site scripting attack. "Adobe strongly urges Adobe Reader users to update to the latest version, Reader 8. Adobe Reader 7 users who wish to stay with their current version can follow the instructions outlined in the bulletin," Adobe advised. Adobe also issued recommendations for a server-side workaround for Website operators.
- Source: <http://www.networkworld.com/news/2007/011007-adobe-patches.html>

29. *January 09, US-CERT* — **Technical Cyber Security Alert TA07-009A: Microsoft Updates for Multiple Vulnerabilities.** Microsoft has released updates to address vulnerabilities that affect Microsoft Windows, Internet Explorer, Outlook, and Excel as part of the Microsoft Security Bulletin Summary for January 2007. The most severe vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on a vulnerable system. Microsoft has provided updates for these vulnerabilities in the January 2007 Security Bulletins. The Security Bulletins describe any known issues related to the updates. Note any known issues described in the Bulletins and test for any potentially adverse affects in your environment.
- Microsoft Security Bulletin: <http://www.microsoft.com/technet/security/bulletin/ms07-jan.mspx>
- Source: <http://www.uscert.gov/cas/techalerts/TA07-009A.html>

30. *January 09, US-CERT* — **Technical Cyber Security Alert TA07-009B: MIT Kerberos Vulnerabilities.** The MIT Kerberos administration daemon contains two vulnerabilities that may allow a remote, unauthenticated attacker to execute arbitrary code. US-CERT is aware of two vulnerabilities that affect the Kerberos administration daemon: Kerberos administration daemon fails to properly initialize function pointers and Kerberos administration daemon may free uninitialized pointers. These vulnerabilities are addressed in MIT krb5 Security Advisory 2006-002 and MIT krb5 Security Advisory 2006-003. Patches for these issues are also included in those advisories.
- Source: <http://www.uscert.gov/cas/techalerts/TA07-009B.html>

Current Port Attacks	
Top 10 Target Ports	The top 10 Target Ports are temporarily unavailable. We apologize for the inconvenience. 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

31. *January 10, Miami Herald* — Package at Florida recruiting office draws bomb squad.

Police in North Miami Beach investigated a suspicious package left behind at the U.S. Navy Recruiting Office on Wednesday morning, January 10. Police say a man walked into the office just after 10:30 a.m. EST and made a comment about the war in Iraq. He then stepped outside and left a package by the door. The man snapped a photo of the building before walking away, police said. North Miami Beach police closed off the street between Northeast 10th and 15th avenues. Bomb squads from the Miami-Dade Police Department and the FBI soon followed. Investigators later decided it posed no threat to public safety.

Source: <http://www.miami.com/mld/miamiherald/16428083.htm>

[[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.