



Department of Homeland Security Daily Open Source Infrastructure Report for 18 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

- The Department of Homeland Security announced on Wednesday, January 17, that it will launch the DHS Traveler Redress Inquiry Program, an easy to use, single point of inquiry for travel-related issues. (See item [17](#))
- USA TODAY reports a long-delayed program aimed at speeding trusted travelers through airport security took a big step Tuesday, January 16, when it opened at one terminal in New York's John F. Kennedy International Airport, the first besides Orlando International Airport. (See item [19](#))
- The Associated Press reports hundreds of people were in emergency shelters and thousands remained in darkened homes after a winter storm that left 54 dead in nine states from Texas to Maine. (See item [38](#))

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 17, Scotsman (Scotland)* — **Armed police move in at energy sites.** Armed police were deployed for the first time Tuesday, January 16, at two key oil and gas facilities in Scotland following a government review of potential terrorist targets. The officers from the

Ministry of Defense police force have begun foot and mobile patrols at the St Fergus gas terminal, near Peterhead, and the Garlogie gas compressor station in Aberdeenshire. Armed guards have also been stationed at two vital infrastructure sites in England — the Bacton terminal in Norfolk and the Easington terminal, on Humberside. The deployment is scheduled to last until 31 March. The Home Office declined to reveal why the four specific sites in the UK had been chosen for the heightened security precautions, but insisted the deployment was not the result of a specific terrorist threat. Seven armed officers will be on duty at any one time at St Fergus, which processes natural gas to serve about a fifth of Britain's daily gas production from more than 20 fields. Superintendent Dennis Jackson said that the decision to deploy armed officers to guard the key installations was "realistic" in view of the ongoing threat from international terrorism.

Source: <http://news.scotsman.com/scotland.cfm?id=85642007>

2. *January 17, Reuters* — **Solar power eliminates utility bills in U.S. home.** Michael Strizki heats and cools his house year-round and runs a full range of appliances including such power-guzzlers as a hot tub and a wide-screen TV without paying a penny in utility bills. His conventional-looking family home in the pinewoods of western New Jersey is the first in the United States to show that a combination of solar and hydrogen power can generate all the electricity needed for a home. The Hopewell Project comes at a time of increasing concern over U.S. energy security and worries over the effects of burning fossil fuels on the climate. Strizki runs the 3,000-square-foot house with electricity generated by a 1,000-square-foot roof full of photovoltaic cells on a nearby building, an electrolyzer that uses the solar power to generate hydrogen from water, and a number of hydrogen tanks that store the gas until it is needed by the fuel cell. New Jersey's utility regulator supported the project because it helps achieve the state's renewable-energy goals, said Doyal Siddell a spokesperson for the agency. The project also got equipment and expertise from a number of commercial sponsors including \$50,000 worth of batteries and stainless steel piping costing around \$28,000.

Source: http://www.boston.com/business/technology/articles/2007/01/17/solar_power_eliminate_utility_bills_in_new_jersey_home/

3. *January 16, Star Tribune (MN)* — **Nuclear plant at Monticello shut down indefinitely.** The Monticello nuclear power plant, located about in Minnesota, 45 miles northwest of the Twin Cities, remains shut down indefinitely, as an investigation continues into why a large metal component broke loose inside the plant, federal officials said Tuesday, January 16. A 35,000-pound control box fell off a steel beam inside the plant last Wednesday, triggering safety systems that shut down the nuclear reactor automatically. The incident was outside the reactor, and no radiation was released. Jan Strasma of the Nuclear Regulatory Commission said, "The initial assessment is that the welds broke due to vibration over the years," and one side of the box dropped about a foot onto a large steam pipe. The mechanisms inside the box apparently malfunctioned and opened valves in four other steam pipes, which activated sensors that shut the plant down immediately. David Lochbaum of the Union of Concerned Scientists said that even though the sensors at Monticello worked successfully last week, it can be risky to rely too much on a nuclear plant's automatic shutdown system. Aging nuclear plants could face additional stress if utilities try to run them too long between maintenance shutdowns, or boost their power output beyond what they were designed to produce.

Source: <http://www.startribune.com/462/story/940767.html>

4. *January 16, Parksville Qualicum News (Canada)* — **Vandals shoot three transformers.** The Royal Canadian Mounted Police (RCMP) are looking for information about who was responsible for shooting out three BC Hydro transformers in the Errington area in British Columbia, Canada. The RCMP said someone blew out two transformers with a shotgun on January 10. A third transformer has since been found in similar condition on the same road. Source: <http://www.pqbnews.com/portals-code/list.cgi?paper=50&cat=23&id=811829&more=>

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

Chemical Industry and Hazardous Materials Sector

5. *January 17, Leavenworth Times (KS)* — **Resident taken to hospital after carbon monoxide exposure.** One person was taken to the hospital for symptoms related to carbon monoxide exposure after firefighters found the dangerous substance Tuesday, January 16, in a Lansing, KS, home, according to a fire department spokesperson. Chief Rick Huhn said firefighters found a CO reading of 46 parts per million in the home's furnace room. There was a reading of 11 parts per million elsewhere in the residence. An adult and two children were at home at the time. Huhn said the symptoms were similar to those of a cold. Huhn said the residents were told to get out of the house to avoid additional exposure and have a repair person check the furnace right away. Source: http://www.leavenworthtimes.com/articles/2007/01/17/news/new_s05.txt
6. *January 16, News Gazette (VA)* — **Propane leak at Kerrs Creek Amerigas storage facility.** Close to 6,900 gallons of propane leaked from an 18,000-gallon tank Tuesday, January 16, at the Amerigas storage facility on U.S. 60 west in Kerrs Creek, VA, before company repairmen were able to replace a faulty valve. Robert Foresman, deputy director of emergency management for Rockbridge County, said workers at the site discovered the leak around 2 p.m. by hearing the gas escape from the defective valve. Traffic was blocked on U.S. 60 while workers from Amerigas inserted a plug into the defective valve to stop the leak and then replaced the valve with a new one. Foresman said the windy day alleviated some of the potential danger of the situation by dispersing the gas. On warm, quiet days, the gas that is heavier than air will settle on the ground. As with other fuels, it is toxic to inhale the fumes of propane. Lexington and Kerrs Creek fire departments responded to the call as did the Lexington Rescue Squad. Source: http://www.thenews-gazette.com/articles/2007/01/17/breaking_news/breaking1.txt

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

Defense Industrial Base Sector

7. *January 17, Government Accountability Office* — **GAO-07-234: DoD's High-Risk Areas: Progress Made Implementing Supply Chain Management Recommendations, but Full Extent of Improvement Unknown (Report).** Military operations in Iraq and Afghanistan have focused attention on the Department of Defense's (DoD) supply chain management. The supply chain can be critical to determining outcomes on the battlefield, and the investment of resources

in DoD's supply chain is substantial. In 2005, with the encouragement of the Office of Management and Budget (OMB), DoD prepared an improvement plan to address some of the systemic weaknesses in supply chain management. The Government Accountability Office (GAO) was asked to monitor implementation of the plan and DoD's progress toward improving supply chain management. GAO reviewed (1) the integration of supply chain management with broader defense business transformation and strategic logistics planning efforts; and (2) the extent DoD is able to demonstrate progress. In addition, GAO developed a baseline of prior supply chain management recommendations. GAO surveyed supply chain-related reports issued since October 2001, identified common themes, and determined the status of the recommendations. GAO recommends that DoD complete its logistics strategy and develop and implement outcome-focused performance metrics and cost metrics for supply chain management. DoD concurred with GAO's recommendations.

Highlights: <http://www.gao.gov/highlights/d07234high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-234>

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

Banking and Finance Sector

8. *January 17, Sophos* — **UK 070 numbers exploited by e-mail lottery scammers.** SophosLabs has revealed that British 070 numbers are the second most commonly used telephone numbers in these scams. U.S.-based telephone numbers top the list. Known as "personal numbers", 070 numbers look like mobile phone numbers, but can actually be easily redirected to any number anywhere in the world. In addition, 070 numbers can be acquired for free, as higher charges are paid by the caller to use them. "Internet scammers are scooping up these free 070 personal phone numbers, redirecting them overseas, and posing as British lottery officials. They can easily cycle through a bunch of these 'throw-away' numbers, using them to con innocent victims into revealing confidential information that can then be used to empty bank accounts and commit identity theft," said Graham Cluley of Sophos. Many new lottery scams using 070 personal numbers are seen each day. "With 070 numbers, callers have no way — short of persuading the 070 service provider to tell them — to determine where their call ends up. They may think they are speaking to an official in London, when really they're on the phone to a scammer in Lagos," continued Cluley.

Source: http://www.sophos.com/pressoffice/news/articles/2007/01/070s_cam.html

9. *January 17, Sophos* — **Researchers mismanage MySpace phishing scam and put thousands at risk.** Several media reports indicate that MySpace users are the latest victims of a phishing scam. Approximately 60,000 users were recently targeted and directed to a scam page, which mirrored MySpace's login page. Unknowing users entered login and password credentials, which were then sent off to scammers. In this case, the intent was not overtly malicious. Those responsible were supposedly bringing to light security flaws present in popular Web browsers. The fallout, however, did not stop there. The whistleblowers took their act a step further by publicly directing others to the stolen information online. By exposing the logins and passwords, thousands of innocent people, many of whom are young adults, are now at risk for identity theft or worse. Stated Ron O'Brien of Sophos, "By directing people to this information, not only have these individuals put people at risk for identity theft, but they have armed criminals and deviants with direct access to thousands of individuals."

Source: http://www.sophos.com/pressoffice/news/articles/2007/01/mysp_acephish.html

10. *January 17, Washington Post* — **Vast data collection plan faces big delay.** The Treasury Department reported to Congress Tuesday, January 16, that a data-collection program to give counterterrorism analysts routine access to as many as 500 million cross-border financial transactions a year could not be implemented until 2010. The department had hoped to implement it by the end of this year. The Cross-Border Electronic Funds Transfer Program was part of the 2004 Intelligence Reform Act, and Congress directed the Treasury secretary to determine if the program would be effective in tracking terrorist financing. In a report to Congress that was scheduled to be released Wednesday, the Treasury Department concluded that the program was technologically feasible and has value, but said it needs to determine whether the counterterrorism benefit outweighs banks' costs of compliance and to address privacy concerns. Banks and money services are required by law to keep records on all wire transfers of \$3,000 or more. The proposed program would mandate that each of those transactions — if they cross the U.S. border — be reported to the Treasury Department's Financial Crimes Enforcement Network (FinCEN).

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/16/AR2007011601576.html>

11. *January 16, Des Moines Register (IA)* — **Fake checks fool Iowans in lottery scams.** Con artists are conducting a wave of counterfeit-check lottery scams that are cheating Iowans out of thousands of dollars when they try to claim jackpot prizes, Iowa Attorney General Tom Miller said Tuesday, January 16. One case last week involved a northern Iowa woman who had wired \$3,500 for “processing fees and taxes” to try to collect a \$175,000 “lottery prize” Another case involved an eastern Iowa man who lost \$2,900 in “taxes and administration fees” in an attempt to collect a \$50,000 “prize.” “This is a nasty consumer fraud that is rampant across the state,” said Miller. The scams have become increasingly sophisticated, using the names of real lotteries and well-known logos such as that for the Powerball game. Most of the scam victims are initially skeptical, Miller said, but their guard goes down when the bank provides the funds from the check, and their hopes get high for a windfall. The counterfeit checks are extremely well done, and can even fool bank tellers, he said.

Source: <http://desmoinesregister.com/apps/pbcs.dll/article?AID=/2007/01/16/NEWS/70116022/1001/NIE>

12. *January 16, Journal News (NY)* — **Westchester library used in money-laundering scheme.** Federal prosecutors have lodged money laundering charges against Stephen Eric Lawrence and John David Lefebvre for transferring billions of dollars in illegal online gambling proceeds to overseas companies. The arrests followed a seven-month investigation that included use of a computer terminal at an unnamed Westchester County, NY, public library. The U.S. Attorney's Office and the FBI said the two men transferred billions in gambling dollars through Neteller PLC, an online payment services company they founded in 1999. In 2005, the company reported \$7.3 billion in financial transactions and net profits of \$91.5 million.

Source: <http://www.nyjournalnews.com/apps/pbcs.dll/article?AID=/2007/01/16/NEWS02/701160408>

[[Return to top](#)]

Transportation and Border Security Sector

13. *January 17, Associated Press* — **Train blaze continues to burn in Kentucky.** Thick, billowing smoke and flames fed by volatile chemicals leaking from a derailed train belched into the sky early Wednesday, January 17, frustrating officials long after the accident shut down a highway and forced evacuations. With water appearing to be of little use in putting out the flames, fire officials expected it would burn out by Wednesday morning and then cleanup operations could begin. "The amount of water that we're flowing is just ungodly, and it's not making a lot of headway, to be quite honest," said Rob Orkies, fire chief of the Zoneton Fire District in Bullitt County. Firefighters used 2,000 gallons of foam, including a large quantity from a nearby chemical factory, from late Tuesday to Wednesday morning. "It's a better weapon of choice," Major Garry Key of the Zoneton Fire Department said. Despite the efforts of 60 firefighters, Key said the blaze remained out of control at 6 a.m. EST.
Source: http://www.nytimes.com/aponline/us/AP-Kentucky-Train-Fire.html?_r=1&oref=slogin
14. *January 17, Gannett News Service* — **Train derails in East Rochester.** A crane was brought to the scene of Tuesday night's, January 16, train derailment in East Rochester, NY, that sent freight cars tumbling off an overpass and into front yards. Mayor David Bonacchi said there was no indication that anyone was hurt or killed in the accident. About 150 area customers were without power initially because of the accident, said Rochester Gas and Electric spokesperson Dick Marion. An additional 450 lost power when homes had to be de-energized for safety. Crews planned to work throughout the night to restore power. The westbound train with about a dozen cars was headed from Syracuse to Buffalo and traveling about 60 mph when it left the tracks about 7 p.m. EST. Officials said all but the locomotives left the tracks. CSX spokesperson Gary Sease said the mainline tracks would be shut down for some time as investigators clear the wreckage and attempt to determine the cause of the derailment.
Source: <http://www.star-gazette.com/apps/pbcs.dll/article?AID=/20070117/UPDATE/301170001/1001/NEWS>
15. *January 17, New York Sun* — **Train carrying propane derails in Queens.** A train carrying thousands of gallons of propane gas derailed at a Queens, NY, rail yard on Tuesday, January 16, prompting nearby businesses to evacuate the area. Officials said the train derailed around 9 a.m. EST, when the operator was backing the 10-car freight train into Maspeth Train Yard near Metropolitan Avenue in Maspeth, NY. Officials speculated that he may have gone too far, causing one of the cars to slip off the tracks. No leaks were reported from that car, which reportedly was holding some 30,000 gallons of propane. Meanwhile, dozens of people were evacuated from nearby businesses and homes as the Fire Department and other city agencies worked to restore the train to the tracks.
Source: <http://www.nysun.com/article/46816>
16. *January 17, Washington Technology* — **Skinner: DHS financial systems lack strong security.** The Transportation Security Administration (TSA) has inadequate computer security controls on its financial systems, according to a new report released on January 17, by Homeland Security Department Inspector General Richard L. Skinner. The special report is a letter from KPMG LLP accounting firm on IT matters related to TSA's fiscal 2005 financial statements. KPMG was hired to audit the TSA's finances; however, it did not complete its audit

because it did not receive final financial statements from the agency. The letter was released in a redacted form with sensitive portions blacked out. It found continuing IT control weaknesses that put at risk the confidentiality, integrity and availability of critical data.

Report: http://www.dhs.gov/xoig/assets/mgmttrpts/OIGr_07-18_Dec06.pdf

Source: http://www.washingtontechnology.com/news/1_1/daily_news/29998-1.html?topic=homeland

- 17. *January 17, Department of Homeland Security* — **DHS to launch Traveler Redress Inquiry Program.**** The Department of Homeland Security (DHS) announced on Wednesday, January 17, it will launch the DHS Traveler Redress Inquiry Program (DHS TRIP), an easy to use, single point of inquiry for travel-related issues. DHS TRIP was developed to provide a central gateway to address watch list misidentification issues, situations where individuals believe they have faced screening problems at immigration points of entry, or have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at the nation's transportation hubs. DHS TRIP will share information it receives with the Department of State and airport and airline operators, as needed, to resolve issues. DHS TRIP will function in accordance with the routine uses identified in the applicable Privacy Act System of Records Notice (SORN) which, along with the NPRM, has been submitted to the Federal Register and will soon be published.

To view the SORN and the NPRM, see <http://www.regulations.gov/>

Source: http://www.dhs.gov/xnews/releases/pr_1169062569230.shtm

- 18. *January 17, KLTV 7 (TX)* — **Nine-year-old runaway steals car, sneaks on flight to Texas.**** Southwest Airlines says a nine-year-old Washington boy with a history of stealing cars and running away sneaked onto a plane bound for Texas — only to get caught after flubbing an airport connection. Semaj Booker is a fourth-grader from Lakewood, WA. Police say Semaj apparently found a boarding card and made it through airport security on Tuesday, January 16, hopping two separate flights but landing in San Antonio — short of his Dallas destination. He had been trying to get to his grandfather in Dallas, where he used to live. Booker remained in juvenile custody today in San Antonio. The boy was unhappy after his family moved to Lakewood.

Source: <http://www.kltv.com/Global/story.asp?S=5951695>

- 19. *January 16, USA TODAY* — **Registered Traveler starts at JFK airport.**** A long-delayed program aimed at speeding trusted travelers through airport security took a small but dramatic step Tuesday, January 16, when it opened at one terminal in New York's John F. Kennedy International Airport (JFK). The opening marks the official launch of Registered Traveler beyond Orlando International Airport, which since July 2005 has run the only airport-sponsored program to put airline travelers at the front of security lines if they pay about \$100 a year and pass a background check. Many airlines give first-class and other preferred passengers their own line leading to security checkpoints. Registered Traveler opens such privileges to a potentially much wider market. Indianapolis International Airport plans to start a Registered Traveler program Thursday, January 18. Airports in San Jose, CA, and Cincinnati, OH, are scheduled to join next week, said Steven Brill, whose company will manage the programs. More than 30,000 people have joined Registered Traveler at Orlando, FL.

Source: http://www.usatoday.com/travel/news/2007-01-16-registered-traveler_x.htm

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

20. *January 16, United Press International* — Scientists warn of new form of stem rust.

U.S.-based scientists say a new form of stem rust — a virulent wheat disease — has moved from eastern Africa into Yemen and the Arabian Peninsula. Researchers with the Global Rust Initiative and the Agricultural Research Service of the U.S. Department of Agriculture say there's also evidence the disease has spread into Sudan, but more tests are needed to confirm the finding. Until the new findings, the strain of stem rust known as Ug99 had only been seen in Uganda, Kenya and Ethiopia. The last major epidemic of stem rust occurred in North America during the early 1950s and destroyed as much as 40 percent of the continent's spring wheat crop. Scientists plotting the probable trajectory of the new fungus say its spores can be carried over long distances by winds. Models predict if the fungus crossed from eastern Africa to the Arabian Peninsula it could easily spread to the vast wheat-growing areas of North Africa, the Middle East, Pakistan and India.

Source: <http://www.upi.com/NewsTrack/view.php?StoryID=20070116-103756-4197r>

21. *January 16, Canadian Press* — New cases of CWD reported in Canada. More cases of chronic wasting disease (CWD) in wild deer are showing up in Saskatchewan and Alberta, Canada. So far, 30 deer shot by hunters last fall in Saskatchewan have tested positive for the fatal brain malady. More test results are pending. In Alberta, there have been four cases since the fall in areas located just across the Saskatchewan boundary. Officials in both provinces report some of these cases are located in new areas—a finding that suggests the disease may be spreading or that animals with CWD are on the move.

CWD information: <http://www.cwd-info.org/>

Source: <http://www.fftimes.com/index.php/3/2007-01-16/29191>

22. *January 15, Associated Press* — Rules on protecting herds from CWD cost some farmers.

New York's new regulations on preventing the spread of chronic wasting disease (CWD) is costing some farmers. The regulations include higher fencing, increased animal identification and required testing of herds. According to the state, 433 farms care for about 10,000 animals susceptible to the disease. Farmer David Vanderzee says he's spent about \$1.5 million to comply with the rules. Part of that money has gone toward raising miles of fencing at his farm in Washington County.

Source: http://www.capitalnews9.com/content/your_news/north_country/default.asp?ArID=202694

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

Food Sector

Nothing to report.

[[Return to top](#)]

Water Sector

23. *January 17, Associated Press* — Freezing temperatures wreak havoc on water pipes across Southern California. A deep freeze in California has wreaked havoc on the state's urban centers in the form of frozen, broken pipes. Fire departments across Southern California reported receiving hundreds of calls over the last several days about pipes that froze, cracked and burst from the cold. Residents of an apartment complex in Victorville went without water for more than 20 hours because of ruptured pipes. Once repairs were made, the plummeting temperatures caused the pipes to burst again, a building manager said. The Victorville Courthouse was flooded over the weekend when several sprinkler heads froze and broke. Meanwhile, broken irrigation lines may have caused a mudslide that buried a private road in Pasadena under some 150 tons of debris.

Source: http://www.mercurynews.com/mld/mercurynews/news/breaking_news/16479604.htm

[[Return to top](#)]

Public Health Sector

24. *January 17, Reuters* — Egyptian woman tests positive for bird flu. A 27-year-old Egyptian woman has tested positive for the H5N1 bird flu virus, the 19th human case in the most populous Arab country, a World Health Organization official said on Wednesday, January 17. The virus has killed 10 people in Egypt, which has the largest cluster of human bird flu cases outside Asia. Eight other positive cases have recovered since the virus first surfaced in Egyptian poultry in February. The official Middle East News Agency (MENA) identified the woman as Warda Eid Ahmed from the province of Beni Suef south of the capital Cairo. The agency quoted an Egyptian Health Ministry official as saying she has been hospitalized since January 13 with a serious pulmonary inflammation. A health ministry spokesperson said Ahmed had raised hens in her house. The ministry has dispatched a team to take samples from the rest of her family.

Source: <http://www.alertnet.org/thenews/newsdesk/L17812042.htm>

25. *January 17, Guardian Unlimited (United Kingdom)* — Existing drug will cure MRSA, say scientists. Scientists believe they have found a cure for the Methicillin-resistant Staphylococcus Aureus (MRSA) superbug after unearthing an existing drug on a computer database. The discovery means patients could be routinely treated within two or three years, since the drug is known to be safe and is already used on the United Kingdom's National Health Service in the treatment of acute illness. The potentially fatal bug is currently treatable only with the antibiotic vancomycin, and some strains are developing resistance to the drug. A mathematical biologist at Newcastle University, has identified a licensed drug that has been proven to be safe and is no more expensive than existing antibiotics. Professor Malcolm Young has used new computing techniques to identify the combination of proteins that need to be

targeted to kill off MRSA bacteria, and to discover whether a drug targeting these proteins already exists among a list of 10 million compounds.

MRSA information: http://www.cdc.gov/ncidod/diseases/submenu/sub_mrsa.htm

Source: <http://society.guardian.co.uk/health/news/0..1991950.00.html>

- 26. *January 17, Agence France–Presse* — Australia's new year party blighted by disease outbreak fears.** Fears that tens of thousands of New Year revelers in Sydney, Australia, could have been exposed to a potentially fatal illness were raised by health officials. Four middle-aged men who welcomed in the New Year at Sydney's famed harbor fireworks display have been diagnosed with legionnaires' disease, the officials said Wednesday, January 17. The men, in their 50s and 60s, reportedly had nothing in common apart from gathering at the city's main ferry terminal, Circular Quay, on the night of December 31. "We're contacting hospitals and other clinicians to alert them of these cases and to consider the diagnosis in other people's pneumonia, and to report to us if it's a case of legionnaires' disease," said a state health official. Legionnaires' disease causes headaches, fevers, chills, muscle aches and pains leading to respiratory problems and pneumonia.

Source: http://news.yahoo.com/s/afp/20070117/hl_afp/healthaustralia_070117104646

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

Government Sector

- 27. *January 16, Washington Post* — Cutbacks impede climate studies.** The government's ability to understand and predict hurricanes, drought and climate changes of all kinds is in danger because of deep cuts facing many Earth satellite programs and major delays in launching some of its most important new instruments, a panel of experts has concluded. The two-year study by the National Academy of Sciences, released Monday, January 15, determined that NASA's earth science budget has declined 30 percent since 2000. It stands to fall further as funding shifts to plans for a manned mission to the moon and Mars. The National Oceanic and Atmospheric Administration (NOAA), meanwhile, has experienced enormous cost overruns and schedule delays with its premier weather and climate mission. As a result, the panel said, the U.S. will not have the scientific information it needs in the years ahead to analyze severe storms and changes in Earth's climate. Officials from NASA and NOAA said that they had just received the report, which was jointly commissioned by the two agencies to prioritize their efforts over the next 10 years. The review was written by the National Research Council of the congressionally chartered academy and released at the annual meeting of the American Meteorological Society.

Report: <http://www.nationalacademies.org/morenews/20070116.html>

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/15/AR2007011501049.html>

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

Emergency Services Sector

28.

January 17, Washington Post — **Maryland officials credit computer data and traffic stops for crime drop.** Violent crime and property offenses in Prince George's County, MD, dropped nearly 21 percent last year because of a variety of police strategies that included computer analysis of crime trends and increased traffic stops, County Executive Jack B. Johnson and Police Chief Melvin C. High said Tuesday, January 16. Johnson and High attributed the drop to police strategies that they said prevented crime and led to the arrests of career criminals. They also credited the involvement of law-abiding community members who provided officers with information. High said police used computerized data of criminal activity to direct patrol officers and investigators to high-crime areas. Traffic stops have been a particularly effective tactic, said Assistant Chief Roberto Hylton, who heads the patrol bureau. In 2005, county police conducted 52,205 traffic stops; last year, officers made 94,674 traffic stops, an increase of more than 81 percent. Officers often find illegal firearms and drugs during such stops, Hylton said. Officers also sometimes find suspects who are named in arrest warrants, Hylton said.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/16/AR2007011601506.html>

29. *January 16, Iowa City Press-Citizen* — Emergency operators trained in medical aid.

Dispatchers at the Johnson County Sheriff's office in Iowa City, IA, are now trained and equipped to provide emergency medical assistance to callers, Sheriff Lonny Pulkrabek announced Tuesday, January 16. Now when a 911 call comes into the dispatch center, the dispatchers would be able to give the caller additional information to help stabilize the person in need of medical assistance until emergency crews arrive. An example would be giving a caller instruction on how to perform CPR, Pulkrabek said.

Source: <http://www.press-citizen.com/apps/pbcs.dll/article?AID=/2007/0116/NEWS01/70116006/1079>

[[Return to top](#)]

Information Technology and Telecommunications Sector

30. *January 17, IDG News Service* — Dutch prosecutors seek jail time for botnet duo. Dutch prosecutors are pursuing jail terms for two men charged in a large-scale computer hacking scheme in which more than one million computers may have been infected with adware and other malicious programs. The case is the biggest cybercrime case prosecuted so far in the Netherlands, said Desiree Leppens, spokesperson for the organized crime branch of the National Public Prosecution Service in Rotterdam. During a one-day trial that ended Tuesday, January 16, prosecutors showed how at least 50,000 computers were infected by the two defendants, who are 20 and 28 years old. Police have not released their names. The pair used a malicious program called "Toxbot," a worm that can be used to gain remote control of a computer and log keystrokes, prosecutors said.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9008286&source=rss_topic85

31. *January 17, U.S. Computer Emergency Readiness Team* — US-CERT Technical Cyber Security Alert TA07-017A: Oracle releases patches for multiple vulnerabilities. Oracle has released patches to address numerous vulnerabilities in different Oracle products. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and

denial-of-service. Systems Affected: Oracle Database; Oracle Application Server; Oracle HTTP Server (Apache); Oracle Identity Management; Oracle Enterprise Manager Grid Control; Oracle E-Business Suite; Oracle Collaboration Suite; Oracle PeopleSoft Enterprise PeopleTools; Oracle Life Sciences Applications (formerly Oracle Pharmaceutical Applications).

Solution: Apply the appropriate patches or upgrade as specified in the Critical Patch Update — January 2007. Note that this Critical Patch Update only lists newly corrected vulnerabilities.

Oracle Critical Patch Update: <http://www.oracle.com/technology/dep/loy/security/critical-patch-updates/cpujan2007.html>

Source: <http://www.uscert.gov/cas/techalerts/TA07-017A.html>

32. *January 16, CNET News* — **Attack code out for 'critical' Windows flaw.** Computer code that exploits a security vulnerability in Windows has been published on the Internet, making it more urgent for users of the operating system to patch. The attack code exploits a flaw in the way Windows handles Vector Markup Language, or VML, documents, which are used for a type of high-quality graphic on the Web. The bug lies in a Windows component called "vgx.dll" that supports these files. Microsoft provided a fix for the flaw last week with security bulletin MS07-004. At the time, the company warned that it had already seen limited cyberattacks exploiting the vulnerability. However, attack code hadn't been available publicly. On Tuesday, January 16, exploit code was published to a widely-read online security forum. Prior to the public posting of the exploit, other code that takes advantage of the flaw had been made available to users of a security testing tool made by Immunity. However, these attack blueprints are private, supplied to people who pay for the tool.

Source: http://news.com.com/Attack+code+out+for+critical+Windows+flaw/2100-1002_3-6150642.html

33. *January 16, CNET News* — **Google plugs account hijack holes.** Google has patched a cross-site scripting vulnerability in one of its Web-hosting services. If left unpatched, the cross-site scripting (XSS) vulnerability could have allowed hackers to modify third-party Google documents and spreadsheets and to view e-mail subjects and search history, according to the Google Blogoscoped blog. Philipp Lenssen, the author of Google Blogoscoped, a third-party site that comments on Google developments, said the vulnerability was similar to another in Blogger Custom Domains reported on Sunday night. "The security hole is connected to an update to a specific Google service which doesn't correctly defend against HTML injections," he said. According to Lenssen, the earlier Custom Domains vulnerability allowed another Google expert, Tony Ruscoe, to create a page that was hosted on a Google.com domain. Ruscoe was able to prove that he could have used code to steal a user's Google cookie and access their Google services. The second vulnerability, reported by Lenssen, would also have enabled a hacker to use JavaScript code to pass cookie data to an external source.

Source: http://news.com.com/Google+plugs+account+hijack+holes/2100-1002_3-6150578.html

34. *January 16, CNET News* — **Persistent zombie attacks target Symantec corporate software.** Symantec first dismissed the threat, but worm attacks that exploit a known security hole in the company's corporate antivirus tool are proving to be persistent. The attacks target computers running older versions of Symantec Client Security and Symantec AntiVirus Corporate Edition. Compromised systems are turned into remotely controlled zombies by the attacker and used to

relay spam and other nefarious activities. Symantec's Norton consumer software is not affected. "What we have been seeing in December and in the last week and a half is related to new variants of Spybot," Vincent Weafer, senior director of Symantec Security Response, said Tuesday, December 16. "We had a couple of versions of Spybot that went nowhere, but these ones found a way to propagate more effectively." The Spybot variants break into computers through a known security hole in the widely used Symantec antivirus tools. When installed on a PC, Spybot opens a back door in the system and connects to an Internet Relay Chat server to let the remote attacker control the compromised computer. Spybot first surfaced in 2003 and has spawned many offshoots.

Source: http://news.com.com/Persistent+zombie+attacks+target+Symantec++corporate+software/2100-1002_3-6150560.html

35. *January 16, CNET News* — **President signs pretexting bill into law.** It's official: "pretexting" to buy, sell or obtain personal phone records — except when conducted by law enforcement or intelligence agencies — is now a federal crime that could yield prison time. President Bush on Friday, January 12, affixed his signature to the Telephone Records and Privacy Protection Act of 2006. The measure threatens up to 10 years behind bars to anyone who pretends to be someone else, or otherwise employs fraudulent tactics, to persuade phone companies to hand over what is supposed to be confidential data about customers' calling habits.

Source: http://news.com.com/President+signs+pretexting+bill+into+law/2100-1028_3-6150572.html

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	<p>The top 10 Target Ports are temporarily unavailable. We apologize for the inconvenience.</p> <p>Source: http://isc.incidents.org/top10.html; Internet Storm Center</p>
<p>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.</p>	
<p>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/.</p>	

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

Commercial Facilities/Real Estate, Monument & Icons Sector

36. *January 17, Miami Herald* — **Blast forces evacuation of Miami condo.** A chemistry student with a previous arrest for possessing bomb-making materials had to explain to detectives Tuesday, January 16, why he had a horde of chemicals that exploded in his Miami, FL, apartment. Itai Polatnick, 23, may not be charged for Tuesday's blast, which injured no one but displaced dozens of residents. Local and federal law-enforcement agents will work with chemists today to identify and remove the chemicals found inside Polatnick's seventh-floor apartment. Until they do, residents of the 220-unit building won't be allowed into their homes. Many stayed with relatives or elsewhere with help from the American Red Cross. Moss could not confirm Tuesday what chemicals were present, but investigators do not believe the chemicals—many kept in glass jars—were being used to make drugs. Chemicals that Polatnick

stored in a mini-refrigerator exploded, destroying the fridge and blowing away a bedroom wall. The blast set off the building's sprinkler system, flooding the unit underneath Polatnick's.
Source: <http://www.miami.com/mld/miamiherald/16476728.htm>

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

General Sector

37. *January 17, Associated Press* — Russia deploys more police after threat. Russia stepped up security in major cities Wednesday, January 17, deploying thousands of extra police and urging public vigilance a day after officials warned of a possible terrorist threat on public transportation. In Moscow, which was last hit by terrorist attacks in 2004, officials took the unusual step of ordering cell phone service shut off in the subway system. The measure appeared to be an effort to avert the possibility of explosives being detonated by the phones. Uniformed police, some with bomb-sniffing dogs, patrolled subway and train stations as well as other sites around Moscow, checking documents and standing guard at entrances. Public announcements asked passengers to be on alert for suspicious items. Moscow's three main international airports introduced stricter passenger checks and additional police patrols of terminal buildings, news agencies reported. The Kremlin's top official in charge of counterterrorism cooperation, Anatoly Safonov, said the tip-off had come from intelligence agencies of several countries, Interfax reported. Russia cooperates against terrorism with nations around the world, including the United States. The Moscow subway, one of the world's busiest, carries about 8 million passengers a day.
Source: http://www.cbsnews.com/stories/2007/01/17/ap/world/mainD8MN4_2UO0.shtml

38. *January 17, Associated Press* — Storm leaves 54 dead, thousands shivering. Hundreds of people hunkered down in emergency shelters and thousands stuck it out in darkened homes after a winter storm that left 54 dead in nine states. About 320,000 homes and businesses in several states were still without electricity late Tuesday after a storm that brought ice, snow, flooding, and high winds to a swath of the country from Texas to Maine. The Texas Department of Transportation shut down I-10 Tuesday, January 16, from Fort Stockton to San Antonio — a stretch of more than 300 miles. Numerous schools and universities, as well as some local and state government offices, were also closed across the region. Subfreezing temperatures were expected to continue in the state Wednesday, with little sunshine to aid in melting the ice until Thursday or Friday, said National Weather Service meteorologist Kevin Brown.
Source: <http://www.cnn.com/2007/WEATHER/01/17/winter.blast.ap/index.html>

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

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.