



Department of Homeland Security Daily Open Source Infrastructure Report for 26 January 2009

Current Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

- According to USA Today, faulty testing kits from Inverness Medical Innovations in Massachusetts resulted in incorrect diagnoses of West Nile virus in at least 42 states, said an officer with the Centers for Disease Control and Prevention. (See item [25](#))
- WXII 12 Winston-Salem reports that streets near the U.S. Federal Building in Greensboro, North Carolina were closed Friday as crews worked to remove a suspicious package, which was tested and showed positive signs that it contained explosive residue. (See item [28](#))

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams](#)

Service Industries: [Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities](#)

Sustenance and Health: [Agriculture and Food; Water; Public Health and Healthcare](#)

Federal and State: [Government Facilities; Emergency Services; National Monuments and Icons](#)

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 23, Agence France-Presse* – (International) **Gunmen attack two vessels off Nigeria: sources.** Unidentified gunmen Friday attacked two vessels off the Niger Delta, the center of Nigeria's oil and gas industry, a security source said. Around a dozen men in two speedboats attacked a supply vessel about 12 nautical miles off the Bonny oil export terminal. There were no casualties and no one was kidnapped, but some items were stolen, the source said. He said the vessel was sub-contracted by ExxonMobil. The U.S. oil company had no immediate comment. Later, a second vessel came under attack by gunmen in three speedboats, northwest of the Amenam oil field, a Nigerian navy spokesman said. The Amenam facility is operated by French oil company Total.

Source:

http://news.yahoo.com/s/afp/20090123/wl_africa_afp/nigeriaoilunrest;_ylt=AneU3HDc3L9pb5sA18y_90G96Q8F

2. *January 22, Associated Press* – (New York) **Oil barge from NYC hits object, takes on water.** A barge carrying more than 5 million gallons of home heating oil from the New York City area has struck an unknown object and has begun taking on water. No pollution and no injuries have been reported. The U.S. Coast Guard says the commercial tug Meredith C. Reinauer was pushing the barge to Boston on Thursday afternoon when it struck something near Execution Rocks, about a mile north of Sands Point in Nassau County. The master of the tug reported the barge was taking on water. The tug took the barge to anchor off nearby Hart Island. Divers examined the barge’s hull. The Coast Guard confirmed it wasn’t discharging any oil. An oil spill removal company has placed a boom around the barge as a precaution and is transferring the oil to other vessels.
Source: <http://www.newsday.com/news/local/ny-nybarge0123,0,454008.story>
3. *January 21, Science@NASA* – (National) **Severe space weather.** In a NASA-funded study by the National Academy of Sciences entitled Severe Space Weather Events — Understanding Societal and Economic Impacts, experts detailed what might happen to modern, high-tech society in the event of a “super solar flare” followed by an extreme geomagnetic storm. The problem begins with the electric power grid. It is particularly vulnerable to bad space weather. Ground currents induced during geomagnetic storms can actually melt the copper windings of transformers at the heart of many power distribution systems. Sprawling power lines act like antennas, picking up the currents and spreading the problem over a wide area. The most famous geomagnetic power outage happened during a space storm in March 1989 when six million people in Quebec lost power for 9 hours. According to the report, power grids may be more vulnerable than ever. The problem is interconnectedness. In recent years, utilities have joined grids together to allow long-distance transmission of low-cost power to areas of sudden demand. Interconnectedness makes the system susceptible to wide-ranging “cascade failures.”
Source: http://science.nasa.gov/headlines/y2009/21jan_severespaceweather.htm
4. *January 21, KWES 9 Midland* – (Texas) **Heater treater explodes in Midland County.** An energy company is cleaning up a big mess after a heater treater fire in south Midland County, Texas. Firefighters got the call at 3:45p.m. to a tank battery fire on Wednesday afternoon. Fire officials say the fire started after a heater treater exploded. The blast sent the piece of oil field equipment flying about 50 feet and caught the surrounding grass on fire. Volunteer firefighters from Midland County and Greenwood took care of the flames. No one was hurt. The company that owns the equipment, Entergy, is now cleaning up the mess.
Source: http://www.newswest9.com/Global/story.asp?S=9711758&nav=menu505_2

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

Chemical Industry Sector

5. *January 22, Bakersfield Californian* – (California) **FBI raids fertilizer facility.** FBI agents and local hazardous material crews searched a local fertilizer manufacturing facility on January 22 that was fined in 2007 for not reporting the use of hazardous materials. Authorities would not disclose the reason for the search at Port Organic Products Ltd., located west of Bakersfield. KGET Channel 17 reported that agents involved wore protective suits and breathing masks to remove items from a building. Boxes were also taken from an office. County records showed Port Organic Products was fined \$10,000 by environmental health officials in November 2007 following an inspection of the property. By law, companies must file updated inventories with local authorities of hazardous chemicals it stores on-site.
Source: <http://www.bakersfield.com/102/story/671215.html>

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

Nuclear Reactors, Materials, and Waste Sector

6. *January 22, Greenville News Clemson Bureau* – (South Carolina) **NRC: Human error a factor in power and cooling interruption at Oconee Nuclear.** Human error played a part in an interruption of power and cooling at Oconee Nuclear Station near Greenville, South Carolina, Duke Energy and U.S. Nuclear Regulatory Commission (NRC) officials said. NRC and Duke officials met Thursday to discuss a brief interruption of power and cooling at Oconee's Unit 1 reactor during a scheduled refueling and maintenance outage last April 15. Preliminary NRC findings indicate some safety significance, while Duke contends that the incident was handled properly without compromising safety. A two-second power interruption occurred on the fourth day of the shutdown, while replacing a circuit board on a voltage regulator, said the operations superintendent at Oconee. It was the first time the procedure was being performed on the regulator that had been replaced in the previous refueling outage, 18 months earlier, he said. A breaker trip setting was not correctly set, and a resulting sequence of reactions led to the loss of coolant. Human error also was cited in the preparation of the maintenance procedure, by not recognizing that equipment would react to the sequence of events as it did, Duke and NRC officials said. NRC officials also mentioned that an alarm on a computer in the control room indicating the loss of coolant was missed by operators.
Source:
<http://www.greenvilleonline.com/article/20090122/NEWS01/90122021/1004/NEWS01>
7. *January 22, Reuters* – (New Jersey) **Exelon gives NRC data on NJ Oyster Creek renewal.** Exelon Corp. submitted an analysis Thursday to the U.S. Nuclear Regulatory Commission (NRC) showing the drywell shell at Oyster Creek in Ocean County, New Jersey is thick enough to help ensure the continued safe operation of the nuclear power reactor for an additional 20 years. The condition of the drywell is the subject of a contention by a citizens group opposed to the relicensing. In a release, Exelon said the nearly 400-page summary of the 3D analysis shows the drywell shell has adequate safety margins in excess of those required by the American Society of Mechanical Engineers Code. Exelon is waiting for the NRC commissioners to make decisions on the renewal application and a company proposal to regularly inspect the drywell.
Source: <http://www.forbes.com/afxnews/limited/feeds/afx/2009/01/22/afx5953454.html>

8. *January 22, News Journal* – (New Jersey) **PSEG releases safety report for Salem 1 plant.** The U.S. Nuclear Regulatory Commission (NRC) has noted three “very low safety significance” problems at the Salem 1 nuclear plant near Salem, New Jersey after an investigation triggered by a cooling system control failure in October. Federal officials began the review after PSEG Nuclear reported that, for more than eight hours, it was unable to determine water levels in a cooling system that keeps one of the reactor cooling systems pressurized. An NRC spokesman said none of the findings resulted in citations against PSEG. The report was released Wednesday. Investigators said there was no danger to the public during the cooling water problem, and that no “unusual incident was declared,” although water levels had fallen to 16.6 percent of the total amount at a time when a level indicator showed 80 percent. The problem resulted from shutdown activities and chemical processes that distorted water level readings without being noticed by operators, the NRC concluded.
Source: <http://www.delawareonline.com/article/20090122/NEWS08/901220338>
9. *January 22, U.S. Nuclear Regulatory Commission* – (Florida) **Positive fitness for duty test.** At the Turkey Point nuclear power plant near Miami, Florida, a non-licensed contract supervisor had a confirmed positive for alcohol during “for-cause” fitness-for-duty test. The contractor’s access to the plant has been terminated. The licensee notified the U.S. Nuclear Regulatory Commission resident inspector.
Source: <http://www.nrc.gov/reading-rm/doc-collections/event-status/event/2009/20090123en.html#en44798>
10. *January 21, Reuters* – (Pennsylvania) **Exelon shuts Pa. Peach Bottom 3 reactor for work.** Exelon Corp shut Unit 3 at the Peach Bottom nuclear power station in York County, Pennsylvania Wednesday morning to replace a main power transformer, the company said in a release. The company said the replacement was needed to “ensure electricity generated by the plant is delivered reliably.” The transformer is one of three needed to transfer electricity from the plant to the grid. The company did not say when the unit would return to service.
Source: <http://www.forbes.com/afxnews/limited/feeds/afx/2009/01/21/afx5946125.html>

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

Defense Industrial Base Sector

11. *January 23, Space Travel* – (National) **Race to orbit gets underway with Ares-1-X tests.** The first Ares I test rocket, will lift off from Kennedy Space Center, Florida in the summer of 2009. It will climb about 25 miles in a two-minute powered test of Ares I first stage performance and its first stage separation and parachute recovery system. A less obvious — but no less critical — test will be of overall vehicle aerodynamics. The flight of Ares I-X will be an important step toward verifying analysis tools and techniques needed to further develop Ares I, the National Aeronautics and Space Administration’s next launch vehicle. Sensors will measure aerodynamic pressure and temperature at the nose of the rocket, and contribute to measurements of vehicle acceleration and angle of attack. “This launch will tell us what we got right and what we

got wrong in the design and analysis phase,” said a deputy project manager for Ares I-X CM/LAS. The completed two-part flight test article is to be delivered to Kennedy Space Center in early 2009. Before launch, the combined crew module and launch abort system tower will be used to help demonstrate lifting, handling and stacking of Ares I-X flight test vehicle elements. Ares I-X will provide important data for developing Ares I in time to support the vehicle’s critical design review in 2010.

Source: [http://www.space-travel.com/reports/Race To Orbit Gets Underway At Cape With Ares 1 X Test Launch 999.html](http://www.space-travel.com/reports/Race_To_Orbit_Gets_Underway_At_Cape_With_Ares_1_X_Test_Launch_999.html)

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

Banking and Finance Sector

12. *January 23, Medford Mail Tribune* – (Oregon) **Police warn of cell-phone scam.** A scam text message purporting to be from Bank of the Cascades popped up on cell phones across the Rogue Valley — including one issued to the head of the Medford Police Department’s financial investigation section. The message sent out on January 22 asked people to call a number with an area code in California’s Central Valley to verify their accounts as part of a “protection program.” Investigators warned people who got the message on January 22 to delete it without replying or calling the number it provided. Bank of the Cascades reported that it does not conduct business via text messages. The bank’s security division believes this scam is coming from outside the United States.

Source:

<http://www.mailtribune.com/apps/pbcs.dll/article?AID=/20090123/NEWS/901230330>

13. *January 22, PC World* – (International) **Symbian malware takes money from phone.** Hackers have discovered a new way to steal money: texting it out of an individual’s phone. Security vendor Kaspersky Lab says it has spotted new variants of a Trojan horse program that do just that, by taking advantage of a feature that lets mobile-phone users in Indonesia use SMS (Short Message Service) text messages to transfer money in their mobile accounts from one phone to another. The software is a variant of the Trojan-SMS.Python.Flocker malware, originally written by Russian fraudsters. This software had been used to sign unwitting victims up for expensive mobile services such as ringtones, presumably with the program’s authors getting a healthy kickback. For the attack to work, the victim must first be tricked into downloading the Python.Flocker program onto a Symbian-based mobile phone. Once installed, the software uses a feature available to Indonesian mobile-phone users that lets them send a short SMS message to another subscriber that transfers the money into their account. The Trojan transfers the equivalent of between \$0.45 and \$0.90, depending on which version of the program is installed. The Symbian operating system is used in phones made by Nokia, Motorola, Samsung, and Sony Ericsson, among others.

Source:

http://www.pcworld.com/article/158191/symbian_malware_takes_money_from_phone.html

14. *January 22, Waterloo-Cedar Falls Courier* – (Iowa) **Area bank thwarts phishing scam.** A potential Internet phishing scam involving several customers of Grundy National Bank has been quashed, bank officials said on January 21. In this instance, a link to a bogus Web site, designed to simulate the Grundy bank’s legitimate site, was distributed to e-mail accounts. The message came in the form as a “new alert message” and directed the recipient to log into a site designed to resemble the bank’s site. The bank’s marketing officer said the bank received several calls from alarmed customers on January 20 and proceeded to take steps to shut down the bogus site.
Source: <http://www.wfcourier.com/articles/2009/01/22/business/local/10951233.txt>

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

Transportation Sector

15. *January 23, Associated Press* – (International) **Nine injured as Northwest jet hits turbulence.** Eight passengers were hurt and two were taken to local hospitals Thursday morning after a Northwest Airlines jet from Tokyo to Honolulu encountered severe turbulence over Midway Island. One flight attendant also was hurt and was taken to Queen’s Medical Center in serious but stable condition with head and neck injuries, The Airbus A330 landed in Honolulu without further trouble shortly after 8 a.m. local time. The two passengers that were most seriously hurt were transported to Straub Clinic & Hospital with hip, neck, and arm injuries. Medical crews at the airport examined other passengers. Flight 22 carried 285 passengers.
Source: http://www.usatoday.com/travel/flights/2009-01-23-nwa-turbulence_N.htm
16. *January 23, WJAR 10 Providence* – (Rhode Island) **Weight limit changes for Cranston bridge.** The Rhode Island Department of Transportation (DOT) announced a change in the weight limit for the Dyer Avenue Bridge in Cranston. On Friday, January 23, the DOT’s Highway and Bridge Maintenance Division will place barrels to narrow the lanes at the bridge and will put up signs announcing the limit is being lowered to 18 tons or less. The weight limit was lowered due to recent inspections. The bridge is located at Dyer Avenue, less than one-fourth mile north of Park Ave. Approximately 14,200 vehicles travel over the bridge each day.
Source: <http://www.msnbc.msn.com/id/28792892/>
17. *January 22, WIRED* – (National) **As Congress stalls, air traffic creeps toward gridlock.** Congress still has not agreed on how to fund the Federal Aviation Administration (FAA), which means the agency will keep muddling through on a shoestring budget. Another six-month extension would cover the FAA’s operating expenses, but it wouldn’t finance the improvements that must be made. Topping the list is the NextGen air traffic control network that will replace a system built on World War II technology. Getting the \$20 billion system in place is imperative. Without it, the FAA says the nation’s air traffic control system will be effectively gridlocked by 2015. In 2007, the then-FAA administrator proposed a “hybrid funding structure” which would generate revenue based on the costs users impose on the air traffic system. This idea met broad opposition and was abandoned. There has not been much progress since, so it seems the current extension will run out before a reauthorization bill is passed. That is

bad news for an agency with a long list of things that must be done to modernize the nation's aviation infrastructure, which is expected to serve 1 billion people and 15 million flights a year by 2015. NextGen will replace an air traffic control system that uses radar with a network based on Global Positioning System and advanced avionics. The system will allow more efficient tracking of aircraft, increasing efficiency and easing congestion. It is but one item on a to-do list that includes building more runways and repairing decrepit air traffic control towers.

Source: <http://blog.wired.com/cars/2009/01/congress-fails.html>

18. *January 22, KCTV 5 Kansas City* – (Missouri) **Airport workers report suspicious package.** Two workers at an airport cargo facility reported a suspicious package to police on Thursday. The two workers said the package they handled at the Southwest Airlines cargo facility at Kansas City International Airport caused their hands to have a burning sensation. The Kansas City Fire Department's hazardous materials crew was called to the scene. An airport spokesman said the hazmat crew tested the contents of the package and determined that it was a type of glue. The workers did not require any medical attention and returned to work Thursday afternoon.

Source: <http://www.kctv5.com/news/18542647/detail.html>

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

Postal and Shipping Sector

Nothing to report

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

Agriculture and Food Sector

19. *January 23, HealthDay News* – (National) **31M pounds of peanut butter, paste recalled: report.** An estimated 31 million pounds of peanut butter and peanut paste products have been recalled in the ongoing salmonella contamination scare, the Associated Press reported on January 16. As the number of people sickened in the salmonella outbreak approaches 500 in 43 states and Canada, U.S. health officials gave more detail on the scope of the outbreak that has been traced to a now-closed production plant in Blakely, Georgia, owned by Peanut Corp. of America. The U.S. Food and Drug Administration (FDA) reported on January 22 on its Web site that its investigation has determined that Peanut Corp. distributed potentially contaminated products to more than 70 firms, "for use as an ingredient in hundreds of different products, such as cookies, crackers, cereal, candy and ice cream." But products made with peanut butter or peanut paste continued to disappear from store shelves this week, as more than 35 major food producers, retail companies, specialty companies and pet food suppliers issued precautionary recalls. The flood of recalls followed an FDA warning last weekend that consumers should avoid peanut butter products containing peanut butter or peanut butter paste while the widespread salmonella outbreak probe continued.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2009/01/23/AR2009012301397.html>

20. *January 23, Dairy Reporter* – (National) **FDA’s recall response ‘inadequate’ and ‘ineffective,’ says CSPI.** The Center for Science in the Public Interest (CSPI) has criticized U.S. officials’ response to the peanut butter salmonella outbreak, calling it ‘woefully inadequate’. It said that the relatively long shelf life of peanut products could leave the public at risk of illness unless the FDA acts “effectively to remove contaminated products from stores.” At present, the U.S. Food and Drug Administration can request companies to recall food products voluntarily if it suspects contamination, and provides recommendations to firms that initiate their own voluntary recalls. The CSPI said, “Without mandates for recall and few inspectors, the agency’s ability to protect the public is minimal. This latest outbreak proves again that FDA is woefully inadequate to the task of protecting American consumers from unsafe food.” These comments follow a teleconference with reporters on January 21 in which a representative of the FDA put forward the view that the industry itself needs to take its share of responsibility for preventing outbreaks.
Source: <http://www.dairyreporter.com/Publications/Food-Beverage-Nutrition/FoodNavigatorUSA/Legislation/FDA-s-recall-response-inadequate-and-ineffective-says-CSPI/?c=DtqJR18k3Pl5Ijat93Fg6g%3D%3D>
21. *January 23, MedHeadlines* – (National) **FDA says no to labels on food from genetically engineered animals.** In a recent announcement, the U.S. Food and Drug Administration (FDA) says there is no reason to require labels for foods made from animals that were genetically engineered and sold to American consumers. The animals themselves will require labels designating them as genetically engineered, once such an animal is created that passes the FDA approval process. Thus far, no such animals have met approval for marketing. The announcement was met with controversy. Those in favor of genetic engineering of animals intended as part of the agricultural industry say the genetic manipulation will create livestock that grows faster, produces less toxic waste, and is more resistant to disease. They also claim the foods derived from these animals will be healthier for the consumer. Against using genetically modified animals in the nation’s food supply are those who think altering the molecular structure of these animals comes with the risk of unintended or unimagined long-term consequences.
Source: <http://medheadlines.com/2009/01/23/fda-says-no-to-labels-on-food-from-genetically-engineered-animals/>
22. *January 23, Associated Press* – (California) **Calif. farmers curb planting to cope with drought.** Some of the nation’s largest farms plan to cut back on planting crops this spring over concerns that the drought plaguing California will cause federal water supplies to dry up. Farmers in the Central Valley said they would forego planting thousands of acres of canning tomatoes and already have started slashing acreage for lettuce and melons. Computer models of the state’s reservoirs and the year’s patchy snowfall forecast water shortages so extreme that federal officials could cut allotments to zero, managers at the Westlands Water District told their members in an emergency conference call. Officials with the U.S. Bureau of Reclamation and the state Department of Water Resources plan to announce next month how much water they will speed to farms and cities. But farmers say that is too late, since they need to decide what to plant

now, as they negotiate with banks for crop loans. Farmers' decisions to fallow thousands of acres during the 2008 drought cost \$260 million in crop losses statewide, as well as hundreds of jobs. A senior meteorologist with the state water agency said the forecast so far suggests conditions will not improve this spring. "It is pretty clear we are heading into the third dry year in a row," the meteorologist said. "We have only gotten one-third of the rainfall we desperately need, and we are already halfway through the winter."

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/01/22/financial/f163602S93.DTL&feed=rss.news>

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

Water Sector

23. *January 23, San Francisco Chronicle* – (California) **S.F. warned to revamp water system for disaster.** San Francisco must upgrade its emergency water system to avoid a catastrophe like the fire that devastated the city after the 1906 earthquake, according to a report to be released today. Improvements to the system — a network of pipes and storage facilities — will not be cheap, according to the report, which estimates that \$86.7 million is needed to rehabilitate and replace facilities such as pump stations and tanks. An additional \$13.3 million is needed for pipeline improvements, and \$332 million more would be needed to expand the system to the west and south areas of town, the report concludes. The auxiliary water supply system includes pump stations, storage tanks, a reservoir, 172 cisterns, 135 miles of pipeline, and numerous facilities that make it possible to pump water out of the bay. The system allows the Fire Department to draw salt water from the bay and is used only to fight fires, resulting in high water pressure. Yet most of the system, including all of the above-ground facilities and about half of the pipeline, has not been replaced since its construction about a century ago, according to the report.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/01/22/MNGD15FFBN.DTL&tsp=1>

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

Public Health and Healthcare Sector

24. *January 23, Patriot-News* – (Pennsylvania) **Hershey Med infections top state.** Penn State Milton S. Hershey Medical Center had the state's highest infection rate, although it improved from last year. It had 42.8 infections per 1,000 patients, down from 47.8 per 1,000 last year, according to a report released last week by the Pennsylvania Health Care Cost Containment Council. Hershey's infection rate is affected by the fact that it uses electronic infection surveillance considered more accurate than methods used by many hospitals. Still, its rate was higher than comparable hospitals using electronic surveillance. The chief quality officer at the medical center said infection reporting is not standardized, even among hospitals that use electronic surveillance, and that can lead to variations in reported rates. He also said that, in addition to reporting actual infections, the medical center reported "infection markers" that can turn up even without an infection. As an example, a staph infection people often carry on their skin can cause

a marker in a blood test, even though there is no illness, he said.

Source:

<http://www.pennlive.com/news/patriotnews/index.ssf?/base/news/1232683824225931.xml&coll=1>

25. *January 22, USA Today* – (National) **West Nile virus cases were overstated in 2008 across U.S.** State health departments across the nation are learning this month the number of West Nile virus cases they thought they had in 2008 was overstated — in one case by more than 35 percent — because of faulty testing kits. The problem test kits, from Inverness Medical Innovations of Waltham, Massachusetts, resulted in incorrect diagnoses of West Nile virus in at least 42 states, said an epidemic intelligence service officer with the Centers for Disease Control and Prevention (CDC). The CDC raised concerns about the faulty kits. “If a person had a false-positive test result for West Nile virus disease, this may have resulted in the incorrect diagnosis and failure to consider other possible causes of their illness,” the CDC stated on its Web site. A false notion that cases are up also could lead states to alter prevention plans. A spokeswoman said some states may want to adjust their prevention planning once they get the new results. An Inverness spokesman said a component failed in the problem test kits. He added that the problem has been corrected, and the company is working with the U.S. Food and Drug Administration to get the kits back on the market by this spring.
Source: http://www.usatoday.com/news/health/2009-01-22-westnile_N.htm

26. *January 22, KRVN 4 Reno* – (Nevada) **Suspicious packaged detonated at Reno’s VA.** A suspicious package has been detonated at the Reno Veterans’ Affairs Medical Center. It is unknown what the object was, or if it contained explosives. An employee of the VA Sierra Nevada Health Care System reported the object outside the emergency room Thursday morning. Several law enforcement officials were investigating the package, including Reno and Veteran’s Affairs police, the Consolidated Bomb Squad, along with the FBI. While parts of the emergency room have been evacuated, no other areas within the building or surrounding neighborhood have been.
Source: <http://www.msnbc.msn.com/id/28796587/>

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

Government Facilities Sector

27. *January 23, International Herald Tribune* – (International) **Dubai police arrest suspect in U.S. consulate threat.** Police in Dubai have arrested an American citizen suspected of being behind a hoax phone call that prompted the closure last week of the U.S. Consulate over security concerns, a local newspaper reported Friday. The Gulf News quoted Dubai’s police chief as saying that a Lebanese-American man was in custody for making “a malicious report” and claiming the U.S. Consulate in this city-state was under a security threat. The suspect called the authorities twice from a public phone on Tuesday, claiming a Sudanese man was planning to harm the consulate, the police chief said. The U.S. Consulate in Dubai was closed Wednesday to public business after a security alert from local authorities, but the top police official said an investigation found no direct evidence of a threat in the Gulf’s commercial hub.

Source: <http://www.iht.com/articles/ap/2009/01/23/news/ML-Emirates-US-Embassy.php>

28. *January 23, WXII 12 Winston-Salem* – (North Carolina) **Bomb squad removes suspicious package from Federal Building.** Several streets near the U.S. Federal Building in Greensboro, North Carolina were closed Friday as crews worked to remove a suspicious package that had been discovered. Police said the package was tested and showed positive signs that it contained explosive residue. The Greensboro Hazardous Devices Team was called in to remove the package. There were no injuries, and police said roads that had been closed during the investigation were reopened around noon.
Source: <http://www.wxii12.com/news/18549313/detail.html#->
29. *January 23, Martinsburg Journal* – (West Virginia) **Disaster preparedness.** A mock disaster drill that was the first of its kind to be conducted on such a large scale took place Thursday at the 167th Airlift Wing of the West Virginia Air National Guard. The scenario involved the need for a C-5 Galaxy aircraft to make an emergency landing at the 167th base when the crew and passengers fell ill with flu-like symptoms on a returning flight from Afghanistan. According to the drill, it is later determined through a series of tests that those on board have been exposed to anthrax from souvenirs such as rugs and other wool products brought home by the passengers aboard the aircraft. Thursday's drill was unique in that there had never been a scenario involving the presence of a weapon of mass destruction on a C-5, according to Guard representatives. That crew was comprised primarily of representatives from the Center for National Response-Tunnel, the 167th Airlift Wing, City Hospital, Jefferson Memorial Hospital, the health departments in Berkeley and Jefferson counties, Berkeley County Office of Emergency Services, Berkeley County Ambulance Authority and the Eastern Panhandle Chapter of the American Red Cross. Members of the FBI and Customs and Border Patrol in Harpers Ferry also participated in the exercise. Throughout the drill process, a team of 13 evaluators took notes before meeting to discuss and review exceptionally strong or weak points of the mission.
Source: <http://www.journal-news.net/page/content.detail/id/514843.html>

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

Emergency Services Sector

30. *January 23, Chico Enterprise-Record* – (California) **Suspicious duffel bag leads to street closure, evacuation of Chico Police Department.** Chico police headquarters were evacuated about 3:30 p.m. Thursday when a black duffel bag left in the visitors' lobby couldn't be matched to an owner. Workers in nearby office buildings were also advised to evacuate. Humboldt Road was closed for several blocks east of Highway 32 until 6 p.m., when bomb technicians, still unsure of its contents, loaded the bag in a special trailer and hauled it to a remote spot where they intended to explode it open with a water cannon. On Thursday night officials said they knew the bag contained a laptop computer, but had not identified other items.
Source: http://www.chicoer.com/news/ci_11535276

31. *January 22, Alameda Sun* – (International) **Coast Guard search and rescue goes digital.** The Coast Guard and other emergency personnel who respond to distress calls will soon see an improvement in their ability to locate people during search and rescue cases. This improvement centers around an emergency position indicating radio beacon (EPIRB), a device that when activated can act as a virtual lifeline from people in distress to rescue crews by sending out a transmitted signal via air, sea, or land. On February 1, Cospas-Sarsat, an international satellite-based search and rescue (SAR) system established by the United States, Canada, Russia, and France, will cease satellite processing 121.5/243 MHz analog EPIRBs. The SAR will begin processing only the 406 MHz digital radio beacon signals, making it illegal to use the obsolete 121.5/243 MHz beacons. The newest 406 MHz beacons incorporate global positioning system (GPS) receivers that transmit highly accurate positions almost instantly to SAR agencies via the Geostationary Earth Orbit Local User Terminals (GEOSAR) satellites. The digital frequency has been designated internationally for use only for distress. Other communications and interference, such as 121.5 MHz analog signals, is not allowed. The change is expected to result in a substantial reduction in wasted SAR resources on false alerts while simultaneously increasing the responsiveness of the system for real distress cases.

Source:

http://alamedasun.com/index.php?option=com_content&task=view&id=4587&Itemid=10

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

Information Technology

32. *January 23, The Register* – (International) **Countdown to Conficker activation begins.** Security watchers are bracing themselves to respond to the activation of the huge botnet created by the Conficker superworm. The malware has created a network of infected PCs under its control estimated at 9 million or even more, according to the latest estimates — dwarfing the zombie army created by the infamous Storm worm, which reached a comparatively paltry 1m at its peak in September 2007. Variants of Conficker (aka Downadup), which began circulating in late November 2008, exploit the MS08-067 vulnerability in the Microsoft Windows server service addressed by Redmond with an out-of-sequence patch last October 2008. The malware also infects removable devices and network shares using a special autorun file. The worm uses social engineering trickery so that users on Windows machines looking to simply browse the contents of a memory stick may be tricked into selecting an option that actually runs a malware payload and infects their PC.

Source: http://www.theregister.co.uk/2009/01/23/conficker_worm/

33. *January 23, CNET News* – (International) **Apple issues critical QuickTime security update.** Apple issued a critical QuickTime security update, aimed at resolving vulnerabilities in its media player that could potentially allow a malicious attacker to take control of a user's computer, according to an Apple advisory released last week. Users running QuickTime 7 for Windows, or OSX, are affected, as well as those who are using Mac OS X 10.4 or Mac OS X 10.5, according to Apple. Apple is advising users to

update to QuickTime 7.6, with QuickTime 7.6 for Windows, or QuickTime 7.6 for Leopard, or QuickTime 7.6 for Tiger. The update seeks to address QuickTime security flaws which could potentially allow a malicious attacker to launch a buffer overflow and execute arbitrary code on a user's system. The attack could potentially occur via a maliciously crafted movie file, AVI movie file, QTVR movie file, or an RTSP URL, according to Apple. Security researcher Secunia, in its security advisory on January 22, noted the vulnerabilities are considered "highly critical."

Source: http://news.cnet.com/8301-13579_3-10148926-37.html

34. *January 22, Washington Post* – (International) **Pirated iWork software infects Macs with Trojan horse.** A company that makes security software for Mac computers is warning that copies of Apple's iWork productivity software that are available for download from peer-to-peer (P2P) file-sharing networks may be infected with a Trojan horse program. The malicious software appears to be designed to enlist infected systems in a bot army that is targeting Web sites with so much junk traffic they can no longer accommodate legitimate visitors. In an alert issued on January 22, Intego said some pirated versions of the \$79 iWork software suite circulating on BitTorrent trackers are infected with what it calls OSX.Trojan.iServices.A. Intego said the Trojan is bundled so that it runs when the user installs the pirated iWork software. iServices.A then opens up a "backdoor" on the victim's computer, effectively alerting the virus writer that a new system is infected and potentially allowing the attacker to upload new software to or perform other actions on the infected Mac. An Intego spokesperson said it appears from looking at the figures from a high-profile torrent tracker site, as of January 22, the installer program for the infected software suite had been downloaded at least 20,000 times.

Source:

http://voices.washingtonpost.com/securityfix/2009/01/pirated_iwork_software_infects.html?hpid=sec-tech

35. *January 22, DarkReading* – (International) **Trojan attack masquerades as airline e-ticket notice.** Security researchers have spotted a new attack designed to fool users into thinking that airline tickets have been purchased with their credit cards. The attack, which was first spotted as an email from Northwest Airlines, and subsequently as a message from United Airlines, is a realistic-looking "receipt" that contains an attachment bearing the name Your ETicket.zip or eTicket.zip, according to researchers at security vendor Sophos. The idea is to fool the unwitting user into clicking on the attachment to get more information on who purchased it, according to a researcher at Sophos. "The file does not contain a genuine electronic ticket, of course, and your credit card has not been charged," he says. "The hackers are hoping that you will be so affronted at being charged for an airline flight that you have not booked that you will open the attachment without thinking." Users who click on the e-ticket file trigger the download of Troj/Agent-IPS, a data-stealing Trojan horse.

Source:

<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212902049&cid=RSSfeed>

Internet Alert Dashboard

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

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

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

Communications Sector

Nothing to report

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

Commercial Facilities Sector

36. *January 22, Atlanta Journal-Constitution* – (Georgia) **No explosives found after downtown bomb threat.** No explosive device was found after a downtown Atlanta building was evacuated and two Interstate ramps were shut down for about two hours because of a bomb threat on Thursday. An Atlanta police spokesman said a search of the Atlanta Housing Authority offices turned up no suspicious package or device. Police closed the nearby ramps from the Downtown Connector northbound and southbound to Freedom Parkway. Those ramps remained closed until the “all-clear” was sounded about 11:45 a.m. Police also investigated a bomb threat Thursday morning at a Bank of America branch in northeast Atlanta. Nothing suspicious was found at that location either, an Atlanta police spokesman said.

Source:

http://www.ajc.com/metro/content/metro/atlanta/stories/2009/01/22/atlanta_bomb_threat_s.html

37. *January 22, Orlando Sentinel* – (Florida) **Cops, emergency workers stage large hostage-situation drill in Marion County.** What if gunmen overran a Central Florida school, held everyone inside hostage and booby-trapped the building with explosives? Law-enforcement and emergency-response agencies from across the state pondered that possibility Wednesday at a Homeland Security training exercise in Marion County. There, they responded to a mock hostage situation partially inspired by a 2004 incident in Beslan, Russia in which more than 330 people, including 186 children, were killed after being taken hostage at a school. “We’re going from the initial 911 call all the way through the entire incident,” said Seminole County’s emergency manager, adding that the drill was the largest of its kind ever conducted in Central Florida. “This is a chance to see how we all work together,” said a commander at the Orange County Sheriff’s Office. About 100 deputies, their families and students from Lake-Sumter Community College posed as hostages and terrorists. A branch chief for preparedness and response for the O’Gara Group, a security-training firm that helped plan the exercise, said a school-hostage scenario was chosen because schools are relatively vulnerable targets —

they do not have much security — and because terrorists have executed such attacks before.

Source:

<http://www.orlandosentinel.com/news/local/lake/orl-wargames2209jan22,0,888932.story>

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

National Monuments & Icons Sector

Nothing to report

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

Dams Sector

38. *January 23, Lafayette Advertiser* – (Louisiana) **Vermilion receives grant for levees.**

Two federal grants totaling \$93,777 were awarded to Vermilion Parish on Thursday by the Minerals Management Service, one for levees and one for road improvements. The first grant is \$54,277 to close several levee breaches along the North Prong Schooner Bayou. “Hurricane Rita (in 2005) had messed it up and we plugged,” the Vermilion Parish Police jury president said. “Then Hurricane Ike came along and messed it up again.” The levee breaks are allowing salt water to pour into fresh water areas, adding salinity to fresh water that farmers use on their crops, he said. “I remain committed to strengthening coastal defenses to protect our way of life in southwest Louisiana,” a U.S. Representative said. “Salt water quickly destroys our farmland, forcing farmers along the coast to abandon their farms or pay dramatic cleanup costs.”

Source: <http://www.theadvertiser.com/article/20090123/NEWS01/901230310/1002>

39. *January 22, Monitor* – (Texas) **Sinkholes, seeping dams concern water officials.** A

team of researchers is trying to get to the bottom of potential problems at Amistad Dam. The dam, one of two reservoirs that store water for the Rio Grande Valley region, was declared “potentially unsafe” in an inspection report released by the U.S. Section of the International Boundary and Water Commission (IBWC) last year. The report recommended further study and inspections at the dam. Since then, the agency, which oversees reservoirs and levees on the U.S.-Mexico border, has put together a research team that will study the risks at Amistad and make recommendations. Inspectors’ main concern at Amistad, which is in Del Rio, is a cluster of naturally occurring sinkholes in the reservoir, through which water is escaping, the IBWC commissioner said. The team likely will need to look at the geophysics of the dam’s foundation and determine why the sinkholes are occurring, as well as determining where the water is going, officials said. Although the sinkholes are cause for some concern, there is no immediate danger of flooding or breakage, he said. Inspectors also determined that Falcon Dam, northwest of Roma, was “conditionally unsafe” because of concerns about seepage. IBWC is monitoring the reservoir’s levels to determine how much water is being lost. If the agency determines repairs are needed, those will likely take place in 2010, officials said.

Source: http://www.themonitor.com/news/dam_22354_article.html/water_ruth.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 NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421

Subscribe to the Distribution List: Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List: Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

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

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

Department of Homeland Security Disclaimer

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