



Department of Homeland Security Daily Open Source Infrastructure Report for 17 January 2008

Current Nationwide



[For info click here](#)

- According to the Daily Mail, America is considering forcing Britons and other visitors to go through tougher checks when they enter the country, due to the growing threat of terrorists from Europe. The head of the Department of Homeland Security explained that he had no plans to scrap the visa waiver program, but could force Britons and others to register online before traveling. (See items [11](#))
- The Associated Press reported that, in a plan announced Tuesday, more than 300 miles of salmon runs would be restored along the Klamath River. The proposal calls for the removal of four aging hydroelectric dams that have stood on the river for nearly a century; providing electricity for 70,000 customers, but also blocking salmon from reaching their spawning grounds. The proposal must be reviewed by federal agencies and the dams' owner, PacifiCorp, which must agree to their removal. (See item [31](#))

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 16, Philadelphia Inquirer* – (Pennsylvania) **Mine-safety bill sent to Pennsylvania Senate.** A bill revising Pennsylvania's mine-safety law for the first time in 47 years cleared a state senate committee and now heads to the full chamber, which could pass it within two weeks. Approved unanimously yesterday by the Senate

Environmental Resources and Energy Committee, the measure creates a state mine-safety board that can make regulations without waiting for legislative approval; strengthens mine-safety standards; and requires mine operators, rather than employees, to take responsibility for accidents.

Source: http://www.philly.com/inquirer/local/20080116_Mine-safety_bill_sent_to_Pa_Senate.html

2. *January 15, Platts* – (Ohio; Virginia; West Virginia) **FERC clears Columbia plan to expand gas storage capacity.** The Federal Energy Regulatory Commission has approved Columbia Gas Transmission's plan to make key upgrades to gas storage caverns and related facilities in Ohio, West Virginia, and Virginia to boost service to existing customers. Columbia's Eastern Market Expansion, which the pipeline proposed in February 2006, would increase storage capacity on its system by roughly 5.66 Bcf and provide up to 94,000 Mcf/d of storage service deliverability and associated firm pipeline capacity. The company plans to have the new capacity up and running by April 2009.

Source:

<http://www.platts.com/Natural%20Gas/News/6719476.xml?sub=Natural%20Gas&p=Natural%20Gas/News&?undefined&undefined>

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

Chemical Industry Sector

3. *January 15, CBS 7 West Texas* - (Texas) **Odessa chemical plant sets up 9-11 emergency alert system.** Flint Hills Resources has sent a letter to nearby residents in South Odessa, Texas, informing them about a new warning system they have put in place in case of emergency. In an effort to be a good neighbor Flint Hills Resources wants to warn Odessans about flaring, which creates a bright flame while burning off built up hydrocarbons. "Sometimes there's loud noises, black smoke associated with that, because of that we know it can be concerning to the community," said the plant manager. That is why the chemical plant is working with the City of Odessa to send out an automated message to residents through the 9-11 notification system, should a significant flaring event take place. The emergency calls would come between the hours of 10 pm to 6 am. The plant manager said Flint Hills is working to minimize future flares and an emergency call would only be issued if flaring will take place for more than an hour.

Source: <http://www.cbs7.com/news/details.asp?ID=4274>

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

Nuclear Reactors, Materials, and Waste Sector

4. *January 16, Nuclear Regulatory Commission* – (Kansas) **NRC conducting special inspection at Wolf Creek nuclear plant.** The U.S. Nuclear Regulatory Commission is conducting a special inspection at the Wolf Creek nuclear plant in response to problems discovered in a safety system that provides cooling water for the reactor during an

emergency. On January 10, operators discovered pockets of gas in a pipe that should be filled with water. The pipe is part of the emergency core cooling system which provides water to the reactor during an emergency. Workers shut the plant down on January 11 to address the problem. The problem is believed to have been caused by several leaky valves and a pocket of gas that remained in a pipe since the last refueling outage in the fall of 2006. The licensee has vented the gas from the piping and is in the process of restarting the reactor. A two-person team of NRC specialists will review the circumstances related to the problem, the licensee's root cause evaluation, and the effect it had on the operability of the safety system.

Source: http://www.nrc.gov/reading-rm/doc-collections/news/2008/08-006_iv.html

5. *January 15, USA Today* – (National) **NRC plans more security for nuke freight.** The Nuclear Regulatory Commission plans to impose new security requirements on radioactive material shipped across the U.S. that could be an inviting target for terrorists looking to build “dirty bombs.” The effort follows years of criticism from members of Congress, security experts, and environmentalists who say that the commission has not done enough to secure potentially dangerous materials since 9/11 raised fears of attacks. The material is typically shipped to and from medical and industrial sites. The government is particularly concerned about someone stealing or hijacking a truck carrying one of 16 radioactive materials that, in large enough quantities, could be used by terrorists to build radioactive dirty bombs. Some of the materials are used to build sensors and other high-tech gadgets, others are used in cancer treatments. The NRC says the security requirements being considered include contingency procedures if materials go missing, new safeguards for shipment information, new rules on advance notification of shipments, and continuous tracking of shipments through GPS and other technologies. The first of three public hearings on the issue was held Tuesday.

Source: http://www.usatoday.com/news/nation/2008-01-14-Nukes_N.htm?csp=34

6. *January 15, KMBC 9 Kansas City* – (Kansas) **Wolf Creek nuclear power plant still idle.** The Wolf Creek nuclear power plant in southeast Kansas remains idle, five days after operators shut down the facility for what they termed “technical reasons.” A plant spokesperson said inspectors have identified the problem and are working to resolve it. Officials hope to bring the plant back online by Wednesday. The official said the problem concerned a system of pipes that normally carry water to cool the reactor in the event of an emergency. Last Friday, operators discovered that the pipes were full of air and gas instead of water.

Source: <http://www.kmbc.com/news/15054019/detail.html?rss=kc1&psp=news>

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

Defense Industrial Base Sector

7. *January 16, Associated Press* – (National) **SAIC gets \$23M aircraft support contract.** SAIC Inc. said Wednesday it has received a five-year contract for up to \$23 million to provide aircraft support services to the U.S. Navy. The defense contractor will provide aircraft, engine, and equipment support for the Naval Air Systems Command in Patuxent River, Maryland. Work will be related to the E-6B communications platform

that delivers emergency messages to aircraft.

Source: http://biz.yahoo.com/ap/080116/saic_inc_navy_contract.html?.v=1

8. *January 16, Associated Press* – (National) **Raytheon wins \$37.5M Air Force contract.** A unit of Raytheon Co. has won a \$37.5 million Air Force contract to support communications network upgrades for the Minuteman intercontinental ballistic missile system. According to a Defense Department notice released late Tuesday, Raytheon Network Centric Systems will upgrade terminal control functions and other satellite systems for the Minuteman Minimum Essential Emergency Communications Network Program.

Source: http://biz.yahoo.com/ap/080116/raytheon_air_force_contract.html?.v=1

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

Banking and Finance Sector

9. *January 16, Tennessean* – (Tennessee) **Password on laptop had been changed.** A password taped to a laptop stolen from the Davidson County, Tennessee, Election Commission had been changed and could not be used to access voters' Social Security numbers in the computer, a commission official said Tuesday. He said that the laptop had an old password taped on top and one of the laptops was broken. The two laptops that were stolen were to be used during early voting to verify voter identities of the 337,000 registered voters if the main computer system went down.
10. *January 15, Reuters* – (National; International) **N.Y. man arrested in foreign exchange scam.** A New York man, who was sentenced five years ago for his role in a securities fraud scheme, was arrested on Tuesday for allegedly defrauding investors of millions of dollars in a foreign exchange scam. The man, a principal at Razor FX, defrauded hundreds of investors beginning in 2000, telling them he was investing their money in the foreign exchange market when he and his partner were simply putting it in a bank and using it to pay their living expenses, prosecutors said. In the scheme, money put in by new investors was used to pay those who withdrew funds, according to a document prepared by a U.S. postal inspector in support of the application for an arrest warrant. To conceal the scheme, they sent investors false account statements reporting nonexistent trades and profits, prosecutors said. Razor FX had investors in the United States as well as internationally in Canada, Hong Kong, and the United Kingdom. About \$68 million was deposited in one of the firm's bank accounts since it was opened in February 2007, according to the document. Razor FX maintained offices at various times in Great Neck, New York, and Upper Saddle River, New Jersey, and has a Web site. The suspect faces mail fraud and wire fraud conspiracy charges and a maximum of 20 years in prison, prosecutors said.

Source:

http://news.yahoo.com/s/nm/20080115/us_nm/razorfx_arrest_dc;_ylt=AkNidE3.ZGBYrNvMYdFnAXsWIr0F

Transportation Sector

11. *January 16, Daily Mail* – (National; International) **Terror threat from Europe could lead to strict controls on traveling to America.** The growing threat of terrorists from Europe has led America to consider forcing Britons and other visitors to go through tougher checks when they enter the country, according to the U.S.'s head of homeland security. He told the BBC that Europe was increasingly seen as a platform for a potential terror attack in America. He explained that he had no plans to scrap the visa waiver program, but could force Britons and others to register online before traveling. The BBC also reported that a posting to a known Islamic extremist website talked about founding a branch of Al Qaida in the U.K. and killing British politicians, including the prime minister.

Source:

http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=508535&in_page_id=1770

12. *January 15, Associated Press* – (National) **Commuter services brace for possible Amtrak strike.** Unless a long-standing labor dispute between Amtrak and nine unions is resolved by January 30, a strike may take place. There has never been a strike in Amtrak's 36-year history, and it is still likely that one will be averted, either through a last-minute deal or intervention by Congress. If workers do walk out, the 71,000 people who take Amtrak every day will not be the only ones who will suffer. Hundreds of thousands of people who ride commuter trains will join them, since many such services depend on Amtrak employees or infrastructure, particularly in the Northeast. The dispute involves about 10,000 employees whose last contract ended December 31, 1999. After years of unsuccessful mediation, a presidential emergency board issued a report on the dispute December 30, triggering a 30-day countdown until a strike becomes legal. Siding with the unions, the board recommended that wage increases be made retroactive. Amtrak, which relies on federal subsidies, is worried about whether it can afford the back pay. Under the Railway Labor Act, most disputes that get to this point end with a contract based on the emergency board's report. In cases when that does not happen, Congress usually imposes the board's recommendations. The biggest impact of a strike would be felt around New York City, where two major services would be disrupted. Talks between Amtrak and the unions were to resume Wednesday.

Source: <http://www.foxnews.com/story/0,2933,322966,00.html>

13. *January 15, CNN* – (National) **Government touts 'border cards' as passport alternative.** While U.S. citizens will be required to show proof of identification and citizenship at land and sea borders beginning January 31, the truly big changes will occur in June of 2009 when citizens returning to the United States via land and sea will be required to carry passports, just as they are required to when arriving via air today. But there is an alternative. The Department of Homeland Security has approved a number of alternatives for frequent border crossers. First, DHS is working with numerous border states to develop "enhanced drivers' licenses" that would meet

government security requirements and be accepted at border crossings. Washington state's first enhanced license should be issued later this month. Vermont, New York, and Arizona also have signed agreements with DHS, and other states are in discussions, said an official from Customs and Border Protection. The State Department is also developing a passport card -- a wallet-sized card that would be cheaper and more convenient than a passport, but would fulfill the same function at land borders. Passport cards and enhanced drivers' licenses both will have "vicinity radio frequency identification," or RFID chips, which will identify the holders as they approach border checkpoints. The CBP official said the chips will not transmit sensitive information, rather they will contain a unique number that the CBP can use to automatically call up information on the travelers and query law enforcement databases. The number is useless to anyone who does not have access to the government databases, she said. Source: <http://www.cnn.com/2008/TRAVEL/01/15/border.cards/index.html>

14. *January 15, Associated Press* – (National; International) **U.S. warns of 'serious concerns' about Philippine air safety.** The U.S. Federal Aviation Administration has downgraded Philippine airline operations and put them under heightened scrutiny because of their inadequate safety standards, the U.S. Embassy said Tuesday. The decision gives the Philippines a Category 2 rating along with countries such as Bangladesh, Ivory Coast, Ghana, and Indonesia. It means Philippine carriers can continue flying to the U.S. but only "under heightened FAA surveillance," the embassy said in a statement. The embassy also advised Americans flying to and from the Philippines to use carriers from countries whose civil aviation authorities meet international standards. A spokesman for the Philippine Transport Department did not dispute the downgrade and said his department would conduct an in-house investigation to determine the shortcomings and fix them. On its website, the FAA says the Category 2 rating means the country lacks laws or regulations needed for the certification and oversight of airlines under minimum international standards. Source: http://www.usatoday.com/travel/flights/2008-01-15-philippine-safety-warning_N.htm

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture and Food Sector

15. *January 16, Knoxville News Sentinel* – (Tennessee) **Legal fallout follows beef recall.** A \$1 million lawsuit has been filed against Sam's Club and Kansas-based Cargill Meat Solutions. The suit contends that Sam's Club employees assured customers that the frozen ground beef they bought at the membership-based warehouse store was not contaminated, despite media reports of a recall by Cargill. It was only after the plaintiffs cooked the meat and fell ill that Sam's Club employees insist they received a memo

about the E. coli-related contamination, the lawsuit states.

Source: <http://www.knoxnews.com/news/2008/jan/16/legal-fallout-follows-beef-recall/>

16. *January 16, Arizona Republic* – (Arizona) **Leafy-greens producers intensify efforts to keep crops germ-free.** Since the September 2006 E. coli outbreak tied to California spinach that killed three and sickened about 200 people in 26 states, produce growers and shippers, first in California and now in Arizona, have adopted strict standards designed to keep the fields as clean as they can. It has been estimated that the produce industry overall lost about \$1 billion in sales due to that outbreak, which prompted the Western Growers Association to create an agreement that incorporates the latest scientific practices for growing and handling produce. All major shippers in California have signed the agreement. About 40 shippers, representing about 8 percent of the production in Arizona, have signed an almost identical Arizona agreement. For about five months every year, the Yuma, Arizona, area produces an estimated 80 percent or more of the nation's lettuce, spinach, and other leafy produce because it has the acreage and the climate. In the summer, most of the nation's leafy greens come from California. Arizona is less susceptible to bacterial problems, because its produce is grown in the winter, when the soil is cooler and the climate is drier, said a spokesman for the Arizona Department of Agriculture.

Source:

<http://www.freep.com/apps/pbcs.dll/article?AID=/20080116/NEWS07/80116029/1019/BUSINESS06>

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

Water Sector

17. *January 16, Indianapolis Star* – (Indiana) **Water tests conducted near derailment site.** In Indiana, Marion County Health Department workers are testing water in all of the wells identified near the January 6 train derailment site. "We think we have got everyone in our target area, including some people we heard from who were not in our target area, but wanted testing for their peace of mind," said a spokesman. The health department and a contractor hired by CSX will conduct separate tests. Results will be available in about two weeks. Indiana Department of Environmental Management officials estimate about 1,900 gallons of diesel fuel spilled, along with about 27,000 gallons of soybean oil, 21,000 gallons of lubricating oil, and about 1,000 gallons of fertilizer.

Source:

<http://www.indystar.com/apps/pbcs.dll/article?AID=/20080116/LOCAL1804/801160384>

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

Public Health and Healthcare Sector

18. *January 16, Agence France-Presse* – (International) **Bird flu cull begins in eastern India.** Health officials in eastern India began the slaughter of tens of thousands of

chickens Wednesday, a day after New Delhi confirmed an outbreak of the deadly avian flu in the region. The animal resources minister of West Bengal state told AFP that 55 rapid response teams had fanned out from “core areas like Margram where the disease was first detected,” intending to kill more than 400,000 chickens. The slaughter started a day after India’s agriculture ministry confirmed poultry deaths due to avian flu last week in densely-populated West Bengal, which borders Bangladesh, where authorities have struggled to contain an outbreak of the virus. Villagers in Margram said they had sold sick and dead birds for human consumption.

Source: <http://afp.google.com/article/ALeqM5iKz8YfjZk3nOgHIuPSsebQ5OotQw>

19. *January 15, Health Day News* – (National) **Study finds doctors not reporting medical mistakes.** Almost two-thirds of doctors say they are willing to report medical errors, but many of them just do not do it, according to a new study by an associate professor of medicine at the University of Iowa, Carver College of Medicine. His study of 338 doctors from teaching hospitals across the country is published in the January 14 issue of the Archives of Internal Medicine. While 73 percent of the doctors said they would disclose any medical error that caused minor medical harm, and 92 percent said they would report an error that caused major damage, such as death or disability, only 18 percent said they had actually reported minor errors, while only 4 percent said they had made a major error and reported it. Even more troubling, 17 percent acknowledged having made a minor error and not reporting it, while 4 percent indicated having made, but not disclosed, a major error. The occurrence and reporting of medical errors became a major issue in 1999, when the U.S. Institute of Medicine issued a report, *To Err Is Human*, which estimated that the deaths of more than 100,000 Americans are tied to some form of medical mistake.

Source: <http://health.usnews.com/usnews/health/healthday/080115/study-finds-doctors-not-reporting-medical-mistakes.htm>

20. *January 15, Reuters* – (International) **Millions in Brazil seek shots in yellow fever scare.** Millions of Brazilians are lining up at hospitals and clinics to receive yellow fever shots as deaths and suspected cases fuel fears of a resurgence of the deadly disease. The death of a man in Brasilia last week prompted concerns that yellow fever could swamp urban centers, where it was eradicated in the 1940s. More than 20 other suspect cases are being investigated. The government has denied that the country faces an epidemic of yellow fever, which is spread by mosquitoes, but authorities are warning tourists traveling to Brazilian forests, national parks, and rural areas to vaccinate at least 10 days before the trip. More than half of Brazil’s 27 states are partially or entirely considered yellow fever risk areas, including the Amazon and the nation’s capital Brasilia. Most of the coast, which attracts the bulk of tourists, is considered free of the disease. As fears of an outbreak grew among Brazilians all over the country, the Health Ministry gave states more than 3.2 million doses of yellow fever vaccines this year, more than three times the average monthly distribution in 2007.

Source: <http://www.reuters.com/article/latestCrisis/idUSN15407443>

Government Facilities Sector

21. *January 15, WHIO 7 Dayton* – (Ohio) **Bomb threat prompts evacuations at WPAFB.** Security forces at Wright-Patterson Air Force Base evacuated a part of the base as part of an investigation into a bomb threat made to the 445th Airlift Wing about 2:45pm Tuesday. A search of the area is underway and the evacuation order will remain in effect until the area is deemed safe.
Source: <http://www.whiotv.com/news/15056186/detail.html>

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

Emergency Services Sector

22. *January 16, Georgia Tech Research News* – (National) **GTVC: Mapping tool allows emergency management personnel to visually track resources.** According to a statement released today by the Georgia Tech Research Institute (GTRI), a collaborative mapping tool developed by GTRI is helping emergency management officials better coordinate event and incident planning – and real-time response. GTRI has teamed with Atlanta-based Emergency Visions to provide mapping capabilities for a resource database the firm developed to identify, activate, track, and coordinate response assets. The GTRI and Emergency Visions applications were selected by the Florida Division of Emergency Management in June 2007 as part of a solution that combines these comprehensive technology tools with the training and management expertise of a team led by the International City/County Management Association (ICMA). “A lot of mapping systems are pretty complex to operate. Our system was deliberately designed to be easy to use for people who are not mapping experts,” said a GTRI senior research engineer. Researchers began developing the Geographic Tool for Visualization and Collaboration (GTVC) in 2000 for military applications, but it has since been tailored to the needs of the emergency management community and first responders. GTVC can track chemical or smoke plumes and help management personnel plan evacuation routes for emergencies such as hurricanes, fires, or flooding. To do this, the system tracks resources including the locations of hospitals, fire stations, schools, nursing homes, sand bags, dump trucks, water, personnel, and supplies in an affected region. The map can also indicate the status of those assets, such as the number of beds available in a specific hospital.
Source: <http://gtresearchnews.gatech.edu/newsrelease/gtvc-mapping.htm>

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

Information Technology

23. *January 16, IDG News Service* – (National) **Oracle fixes critical flaws in quarterly update.** Oracle Corp. released 26 fixes across its product line in its latest critical patch update, nine of which repair flaws that are remotely exploitable. In an advisory listing the problems, Oracle advised administrators to patch their machines as quickly as possible. Five of the six vulnerabilities in Oracle’s Application Server can be exploited over a network without the need for a username or password, the company said. The

same danger applies to three of seven vulnerabilities in the E-Business Suite and Applications and one of four problems in PeopleSoft Enterprise PeopleTools, Oracle said. In other products, the update includes one patch for Oracle's Collaboration Suite and eight for various database products. Oracle fixed 51 vulnerabilities in its last critical patch update in October.

Source:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9057442&source=rss_news10

24. *January 15, Infoworld* – (International) **Cyber-espionage moves into B2B.** The practice of cyber-espionage is rapidly moving beyond the government sector and finding its way into the world of international business, according to experts with SANS Institute. While the United States and Chinese governments, most notably, have accused each other in recent years of carrying out surreptitious hacking campaigns aimed at stealing strategic information from their respective IT systems -- and many security experts believe that both countries, and many others, are actively engaging in such electronic warfare -- leaders with SANS maintain that the practice has recently begun to spill over into the private sector with greater frequency. According to the training institute's latest research, cyber-espionage efforts funded by "well-resourced organizations" -- including both government-backed and private efforts -- will expand significantly during 2008, in particular as overseas companies look to gain an upper hand in negotiating business deals with large companies based in the U.S. and Europe. In one common scenario, said the director of research for SANS, organizations in the process of establishing legitimate partnerships with such companies are willing to pay hackers to break into those firms' IT systems to gather competitive information to gain an advantage at the bargaining table. More companies than ever before are finding that they have been victimized in such a manner based on the discovery of their sensitive data in the hands of hackers and other fraudsters who have been apprehended by law enforcement officials, the expert contends. "Cyber-espionage is clearly growing across the board. It was much bigger in 2007 than in previous years, and it is expanding slowly into economic espionage involving both businesses and government entities," he said. "This really has a lot of significant implications because people who have never thought of themselves as targets for this type of attack have suddenly become a sweet spot, and many are not prepared to defend themselves."

Source: http://www.infoworld.com/article/08/01/15/Cyber-espionage-moves-into-B2B_1.html

25. *January 15, IDG News Service* – (National) **Flash attack could take over your router.** Security researchers have released code showing how a pair of widely used technologies could be misused to take control of a victim's Web browsing experience. The code, published over the weekend by two researchers, exploits features in two technologies: The Universal Plug and Play (UPnP) protocol, which is used by many operating systems to make it easier for them to work with devices on a network; and Adobe Systems' Flash multimedia software. By tricking a victim into viewing a malicious Flash file, an attacker could use UPnP to change the primary DNS (Domain Name System) server used by the router to find other computers on the Internet. This would give the attacker a

virtually undetectable way to redirect the victim to fake Web sites. For example, a victim with a compromised router could be taken to the attacker's Web server, even if he typed Citibank.com directly into the Web browser navigation bar. "The most malicious of all malicious things is to change the primary DNS server," the researchers wrote. "That will effectively turn the router and the network it controls into a zombie which the attacker can take advantage of whenever they feel like it." Because so many routers support UPnP, the researchers believe that "ninety nine percent of home routers are vulnerable to this attack." In fact, many other types of UPnP devices, such as printers, digital entertainment systems and cameras are also potentially at risk, they added in a Frequently Asked Questions Web page explaining their research. The attack is particularly worrisome because it is cross-platform -- any operating system that supports Flash is susceptible -- and because it is based on features of UPnP and Flash, not bugs that could be easily fixed by Adobe or the router vendors.

Source: <http://www.networkworld.com/news/2008/011508-flash-attack-could-take-over.html>

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: 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

26. *January 15, NetworkWorld.com* – (New York) **Wireless LAN scan finds big security holes in NYC retailers' wireless nets.** There is bad news for some retailers at this week's National Retail Federation trade show in New York City, where WLAN security company AirDefense disclosed the findings of its four-day scan of local retailers' wireless nets. Security for retail wireless nets is still bad, though improving, AirDefense found after scanning nearly 800 stores in the five NYC boroughs between Thursday, January 10, and Sunday, January 13. About one third of the stores had no security at all, not even the minimal encryption provided by the flawed Wired Equivalent Privacy (WEP) protocol. Another third had weak encryption, such as WEP or the pre-shared key mode of the Wi-Fi Protected Access (WPA PSK) specification, which was originally intended as basic security for home or SOHO WLANs. The final third showed a quantum improvement, according to AirDefense's chief security officer: the more advanced WPA2 specification, with 802.1X authentication brought down to every device, including handhelds, on the WLAN, and AES encryption, the strongest commercially available today. "These are the first retail stores we've seen with bulletproof [wireless] security," he says.

Source: <http://www.networkworld.com/news/2008/011508-retailer-wlan-security.html>

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

Commercial Facilities Sector

27. *January 15, Associated Press* – (New Jersey; Kentucky) **1 Dead in explosion at N.J. plant.** An explosion at Tec-Cast, an aluminum castings company located about a mile north of Giants Stadium in Carlstadt, New Jersey, killed one and injured nine others Tuesday morning, authorities said. Workers were performing maintenance on an air pressure vat used to cast molten metals into machine parts, police said. The injured workers were taken to Meadowlands Hospital Medical Center, and Hackensack University Medical Center. About 45 employees were in the building at the time of the explosion. Also on Tuesday, a fire was reported at a BASF Corp. chemical plant that makes pigments for printing, ink, paint, and plastics in west Louisville, Kentucky, forcing employees to evacuate. About 20 employees were in the building at the time, a company spokesman said. No injuries were reported.

Source: http://ap.google.com/article/ALeqM5iz-aMF-d6NOA-iIU_j7JDpKkcjigD8U6GVI00

28. *January 15, KNXV 15 Phoenix* – (Arizona) **Local police firm up security plan for Glendale Super Bowl.** Preparations for the Super Bowl continued Tuesday outside the University of Phoenix Stadium as local law enforcement agencies met to discuss the security plan. The National Football League has traditionally had one agency in charge of security. While host city Glendale has a growing police department with several hundred officers, they admittedly could not handle an event like the Super Bowl by themselves. In an unprecedented collaboration, local, state, and federal agencies will work together, sharing the responsibility for Super Bowl security. They say the plan has won over the initially reluctant NFL. With less than three weeks to go until the Super Bowl, those in local law enforcement say everything appears to be on schedule. Several other developments were unveiled Tuesday, including the announcement that military aircraft will be patrolling the air space over the Valley during Super Bowl week.

Source: http://www.abc15.com/news/local/story.aspx?content_id=d1721717-7597-439f-ad2a-38336ef88499

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

National Monuments & Icons Sector

29. *January 16, Canada Free Press* – (Wyoming) **Yellowstone at risk of hydrothermal explosion, not volcanic.** Yellowstone National Park lies atop one of the world's few dozen hotspots and is home to the Yellowstone Caldera (a volcanic feature formed by the collapse of land following a volcanic eruption) which measures in at 34 miles by 45 miles. Many are now concerned about the hydrothermal activity that the region is known for. Hydrothermal explosions take place when superheated water below the ground's surface, are allowed the room to expand. Once the pressure is removed from the superheated water, it will flash to steam and expand. Given the right amounts of water and the right conditions, such a "flash" could create a substantial explosion. While smaller explosions, mostly harmless to visitors, happen every few years or so, the larger ones occur only about every 700 years. It is these larger ones that have left behind the

world's largest craters as a result of hydrothermal explosions that scientists are trying to understand.

Source: <http://canadafreepress.com/index.php/article/1408>

30. *January 15, World Tribune* – (International) **U.S. intel alerted to threat of ‘Forest Fire Jihad’**. U.S. officials monitoring terrorist web sites have discovered a call for using forest fires as weapons against “crusader” nations. A terrorist website carried a posting that called for “Forest Jihad.” The posting was listed on the Internet on November 26 and reported in U.S. intelligence channels last week. The statement, in Arabic, said that “summer has begun so do not forget the Forest Jihad.” The writer called on all Muslims in the United States, Europe, Russia, and Australia to “start forest fires.” On damage caused by wildfires, the report said that the fires typically take months to put out which means that “this terror will haunt them for an extended period of time.” The fires also will cause economic damage because it will limit exports of timber used to make furniture and also will cause losses to pharmaceutical companies that use trees for ingredients for drugs, the posting said. Smoke caused by the fires will create pollution and military forces could be tied up fighting fires. The post noted that U.S. military forces in Iraq or Afghanistan “could even be recalled” as occurred following hurricane Katrina, which did not occur. “Imagine if, after all the losses caused by such an event, a jihadist organization were to claim responsibility for (starting) the forest fires,” the writer said. “You can hardly begin to imagine the level of the fear that would take hold of people in the United States, in Europe, in Russia, and in Australia.” The post urges terrorists to use sulphuric acid to start a forest fire, as well as gasoline.

Source:

http://www.worldtribune.com/worldtribune/WTARC/2008/me_terror_01_15.asp

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

Dams Sector

31. *January 16, Associated Press* – (Oregon) **Deal would remove Klamath River dams**. More than 300 miles of salmon runs would be restored along the Klamath River as part of a landmark \$1 billion proposal that represents the largest dam removal project in the nation's history. The plan, announced Tuesday, followed two years of closed-door negotiations between farmers, Indian tribes, fishermen, conservation groups, and government agencies battling over the fate of scarce water and fish protected by the Endangered Species Act. The proposal calls for the scrapping of four aging hydroelectric dams that have stood on the river for nearly a century—providing electricity for 70,000 customers, but also blocking salmon from reaching their spawning grounds. The agreement faces significant hurdles. It must be reviewed by federal agencies and the dams' owner, PacifiCorp, which must agree to their removal. The plan contains no provision for paying the estimated \$180 million to remove the dams, leaving that to PacifiCorp. PacifiCorp has previously said it would be willing to remove the dams if its ratepayers do not have to pay. But it has also been pursuing a new 30- or 50-year operating license, which would require it to spend about \$300 million to build fish ladders. Opposition to the agreement is coming from the Hoopa Valley Tribe, based on the Trinity River, which flows into the Klamath below the dams; some farmers who are

not part of the Klamath Reclamation Project; and two conservation groups tossed out of the talks last spring, Oregon Wild and WaterWatch.

Source:

http://www.breitbart.com/article.php?id=D8U6SA3O0&show_article=1&catnum=1

32. *January 16, Sacramento Bee* – (California) **Levee report shocks city.** On Tuesday, the Federal Emergency Management Agency said it would place Sacramento's fast-growing Natomas in a flood hazard zone, essentially halting construction of homes, offices, and stores until the levees are improved. City leaders questioned the evaluation conducted by the U.S. Army Corps of Engineers. They said they would seek "an act of Congress" to stop the federal action and that the new rules could cripple Sacramento's economy. Sacramento is considered the urban area most vulnerable to catastrophic flooding in the nation. In 1998, after an eight-year building moratorium, the corps said the Natomas levees met its minimal 1-in-100 flood protection standard. Then, in July 2006, the corps said the levees did not meet that standard after all, despite the \$57 million in upgrades during the 1990s. On Tuesday, the corps said Natomas levees are not strong enough to withstand even a 30-year storm. Officials at the Sacramento Area Flood Control Agency said Tuesday's announcement will not change their plans for levee upgrades in Natomas. The executive director said his agency has worked closely with the corps to understand its results and changing standards. SAFCA hopes to start construction this summer on the first phase of a \$400 million levee repair project in Natomas. It is designed to restore 100-year protection by 2010, and achieve 200-year protection by 2012. But that project has yet to be approved by state and federal officials, and is subject to a lawsuit.

Source: <http://www.sacbee.com/101/story/637772.html>

33. *January 15, Brownsville Herald* – (Texas) **IBWC to raise levees.** In Texas, work has begun to repair the Rio Grande Valley levee system in Cameron County and is expected to be completed before hurricane season, federal officials said Tuesday. The International Boundary and Water Commission is raising 23 miles of the levee system from Donna to Brownsville by 30 inches in some portions to provide the area with adequate protection from a 100 year flood. Although levee inspections show that it needs improvements, the levee is not in "dilapidated" conditions as has been reported in the media, the IBWC commissioner said. Levee inspections show portions of it have to be filled in because of continuous usage by the public and most recently by an increase of U.S. Border Patrol agents patrolling along the Rio Grande. The plan is to raise the portions that are deficient in order that they meet Federal Emergency Management Agency standards.

Source:

http://www.brownsvilleherald.com/news/levee_83533_article.html/fence_marin.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 NICCRports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389

Subscription and Distribution Information:

Send mail to NICCRports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 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.