



Department of Homeland Security Daily Open Source Infrastructure Report for 30 October 2006

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

- Hackers broke into the computer files of an Ohio hospital over Labor Day weekend, potentially accessing names, addresses, birth dates, and Social Security numbers of about 230,000 patients and their families, as well as a database containing the bank-account information of about 12,000 donors. (See item [8](#))
- A computer security student working on his doctorate has created a Website that allows anyone with an Internet connection and a printer to create and print fake boarding passes for Northwest Airlines flights; officials from the Transportation Security Administration say that using one of these boarding passes would be illegal. (See item [13](#))

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. *October 29, Associated Press* — **Thousands in east without power over weekend.** Thousands of homes and businesses had no electricity Sunday, October 29, from Maryland to Maine as a storm system blasted the region with winds gusting to more than 50 mph, knocking over trees and a construction crane. The storm was blamed for at least two deaths. On Saturday, nearly a quarter-million people in New York City and its suburbs were affected. The worst problems were on Long Island, east of New York City, where 78,683 customers — about 228,000 people — were without power at noon. Utilities in Maine reported 44,000 customers still in the dark at

midday Sunday and gusts up to 50 mph were causing new failures even as crews tried to restore service. New Jersey's Newark Liberty International Airport, one of three major airports for the New York City region, had delays up to 2 1/2 hours, mostly for incoming flights, authorities said. Power failures elsewhere across the region still affected more than two dozen communities Sunday across New Hampshire; 9,500 homes and businesses in Massachusetts; 1,500 customers in Rhode Island; 6,400 in Connecticut; 2,900 in Maryland; 5,000 in New Jersey; 4,700 on New York's Long Island; and 15,500 in upstate New York, state and utility officials said.

Additional source: http://www.iht.com/articles/ap/2006/10/28/america/NA_GEN_US_Storm_Outages.php

Source: <http://apnews.myway.com/article/20061029/D8L2HP500.html>

2. *October 28, Bloomberg News* — **Blackouts await without power upgrade.** New England will need to add power plants capable of generating 4,300 megawatts, and \$3.4 billion of additional transmission investment, by 2015 to avoid blackouts, the region's grid operator, ISO New England, says. The area will need 170 megawatts of new power before the summer of 2009 to assure adequate supplies. "Without the timely addition of new resources, the region will fail to meet established reliability criteria, increasing the possibility of needing to disconnect customers during periods of peak demand," according to the ISO's 2006 Regional System Plan, which was released Friday, October 27. New England currently has proposals to build 37 projects capable of generating 3,871 megawatts, the report states.

ISO Press Release: http://www.iso-ne.com/nwsiss/pr/2006/2006_regional_system_plan_102606.pdf

ISO Report: http://www.iso-ne.com/trans/rsp/2006/rsp06_final_public_version_102606.pdf

Source: <http://www.telegram.com/apps/pbcs.dll/article?AID=/20061028/NEWS/610280340/1002>

3. *October 26, Reuters* — **CL&P energizes power transmission line in Connecticut.** Connecticut Light and Power Co. said it energized the new \$350 million Bethel-to-Norwalk 345-kilovolt electric transmission line in Connecticut on October 12. The utility said the line would allow the delivery of an additional 600 megawatts of electricity to southwest Connecticut and the region, saving consumers about \$100 million annually in federally mandated charges. The line spans some 21 miles to connect CL&P's largest load center, southwest Connecticut, to the region's existing 345-kV energy backbone. The Bethel-Norwalk project is the first of four major initiatives in southwest Connecticut expected to resolve long-standing reliability challenges and will make the regional transmission grid more secure and efficient. In Connecticut, Northeast Utilities and other power companies are working on the Middletown-to-Norwalk project, the Glenbrook Cables project, and the Long Island Replacement Cable, which further extend the benefits of the 345-kV bulk power system into southwest Connecticut.

Source: http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2006-10-26T151323Z_01_N26470808_RTRIDST_0_UTILITIES-NORTHEASTUTILITIES-CONNECTICUT.XML&rpc=66&type=qcna

4. *October 26, Toronto Star (Canada)* — **Hydro One tops in security audit.** The North American Electric Reliability Council (NERC) has given Hydro One top marks for how it runs the province's transmission system, after an intensive two-week audit. NERC found Hydro

One's attention to physical and network security, the agency's training programs, and a high-tech grid-control center as "examples of excellence" other utilities can learn from. It was NERC's first audit of Hydro One since the August 2003 blackout, which originated in Ohio and left more than 50 million people in Canada and the U.S. in darkness. The council's rules and standards were voluntary prior to the blackout. Since the passage of the Energy Policy Act of 2005, however, U.S. utilities are required to comply. Audits are conducted every three years, or annually if a utility is demonstrating weakness in operations. The rules are still voluntary in Canada, but efforts are underway to change that in all the provinces. Stan Johnson, manager of situation awareness and infrastructure security at NERC, said the council received a commitment from Ontario earlier this week, in the form of a memorandum of understanding. He said the standards are expected to be mandatory by year's end, with the rest of the provinces on board by next June.

Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thesar/Layout/Article_Type1&c=Article&cid=1161814211606&call_pageid=968350072197&col=969048863851

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

Chemical Industry and Hazardous Materials Sector

Nothing to report.

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

Defense Industrial Base Sector

5. *October 26, Aviation Week* — **Portfolio approach will govern net-centric acquisition.** The Department of Defense's ongoing experiment with joint capability portfolio management will shape its approach to net-centric system acquisition, according to Deputy Defense Secretary Gordon England. "My suggestion, at least to all of the industry people here today, is that they follow this evolution closely, because this approach will have implications in how we procure our net-centric business services as we go forward," England said during the MILCOM 2006 symposium in Washington Wednesday, October 25. The purpose of joint capability portfolios is to ensure that the capabilities the military is developing will be aligned and interoperable, even if they're spread out over multiple acquisition programs in different services. The Deputy's Advisory Working Group within the Pentagon has selected four test cases for the joint capability portfolio management concept: Joint Command and Control, Battlespace Awareness, Joint Logistics and Joint Net-Centric Operations.

Source: http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/ENG10266.xml

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

Banking and Finance Sector

6. *October 30, MSNBC* — **Financial institutions roll out revamped ATMs, payment card readers.** Two new technologies — contactless credit cards and no-envelope ATMS — are

being rolled out on a grand scale by banks to introduce their customers to the latest payment methods. An embedded radio chip will require the customer to wave the card over a receiver to complete a purchase rather than swiping. Dave Kudrna of Dataflo Consulting said contactless cards could embolden identity thieves. "They don't have to hand a stolen card to a cashier or even show it. You walk up and it never leaves your hand. It's far easier than a fake ID." Banks are also introducing advanced ATMs with no-envelope deposits. With the new technology, the customer doesn't need to key in an amount. Once money is inserted into a slot, the machine sorts, counts, and verifies it. The scanned check images and the total deposit amount appear on the ATM screen. If the consumer experiences a mechanical failure or another problem while making a deposit, the ATM logs a record of the information as well as the machine malfunction.

Source: <http://www.msnbc.msn.com/id/15389063/>

7. *October 28, Denver Post (CO)* — **Identity-theft computer scheme uncovered in apartment search.** An identity-theft scheme that could affect thousands of Americans through misuse of tax records and banking information has been uncovered in Denver, the district attorney's office warned Friday, October 27. Denver police recovered personal and financial information from about 75 individuals and businesses from across the country. The information, which included tax records, bank-account data, online bill-paying records, and other material, appears to have been stolen from computers that were using LimeWire, a file-sharing software program, Lynn Kimbrough, spokesperson for the prosecutor's office, said. Normally, file-sharing software allows only certain types of files, such as pictures or music, to be shared. But the safeguards can be breached and the information stored in the entire computer compromised, Kimbrough said. Kimbrough said that it appears the file-sharing program was exploited to enable someone to illegally access every file and document on computers across the country. Denver investigators are trying to determine if those who downloaded the information simply found computers that didn't have ample security safeguards or managed to breach computer security. Source: http://www.denverpost.com/ci_4564807?source=rss

8. *October 28, Akron Beacon Journal (OH)* — **Children's Hospital data on 230,000 patients, families, 12,000 donors exposed.** Hackers broke into Akron Children's Hospital computer files over Labor Day weekend, potentially accessing names, addresses, birth dates, and Social Security numbers of about 230,000 patients and their families, as well as a database containing the bank-account information of about 12,000 donors. The hospital, located in Akron, OH, began notifying the families on Wednesday, October 25 — seven weeks after the breach was discovered. The hackers gained access to the hospital's computer network during an expansion of the system. Information accessed included billing information from office visits to doctors employed by Children's Hospital. Those records contained personal information, such as Social Security numbers, but did not contain any medical or financial information, the hospital said. The donor database included bank-account information and routing numbers, though it did not contain Social Security numbers. Credit card information attached to the donor files was encrypted. The hospital didn't contact the FBI initially because its security consultants didn't suspect a major problem. Source: http://www.centredaily.com/mld/centredaily/news/nation/15871_658.htm

9. *October 27, Associated Press* — **Shredmobile in New York suburbs.** A \$60,000 mobile paper shredder in New York City's northern suburbs will help residents avoid identity theft,

Westchester County Executive Andrew Spano said. The Shredmobile — basically a white truck with a giant shredder inside — can chop through 75 to 100 pages at once and won't hesitate to shred CDs and floppy disks. Most shredder trucks are built for private companies, but another nearby municipality also offers shredding capabilities. A shredder truck at a community center in the Maryvale neighborhood of Phoenix is part of a program run through the office of Attorney General Terry Goddard.

Source: http://seattletimes.nwsources.com/html/nationworld/2003325647_shred27.html

10. *October 26, CBC News (Canada)* — **IE7 flaw could expose users to phishing attacks.** A reported flaw in the newest version of Microsoft's web browser could leave its users susceptible to fraud attacks of the sort that Internet Explorer 7 (IE7) was built to stop. The vulnerability could allow a scam Website to open a pop-up browser window that contains a faked internet address, exposing IE7 users to potential phishing attempts, according to an advisory issued by Secunia on Wednesday, October 25. The IE7 weakness could let a scammer trick people into thinking they are on a Website that they trust by displaying part of a legitimate address at the beginning of the URL (an acronym for uniform resource locator), Secunia said. "The problem is that it's possible to display a popup with a somewhat spoofed address bar where a number of special characters have been appended to the URL.. which may trick users into performing certain unintended actions," Secunia says. In a post to the Microsoft Security Response Center blog, the company said it is investigating the report and stressed that the browser's built-in tools should block attacks.

Source: <http://www.cbc.ca/technology/story/2006/10/26/tech-ie7flaw-061026.html>

11. *October 26, Websense Security Labs* — **Multiple Phishing Alert: Washington State Employees Credit Union, Nevada Federal Credit Union, Bancolombia, Banca Di Roma.** Websense Security Labs has received reports of several phishing attacks that target banking customers. Each of the phishing e-mails noted below provide a link to a phishing site that attempts to collect user account information.

Washington State Employees Credit Union: Users receive a spoofed e-mail message claiming that their account is about to be suspended. The message tells users that they must verify their online details for their account to remain active.

Nevada Federal Credit Union: Users receive a spoofed e-mail message claiming that they must renew their accounts immediately in order to avoid suspension of their online services.

Bancolombia: Users receive a spoofed e-mail message claiming that the bank servers have been updated and are operative. The email claims that in order to take advantage of new security features, users need to verify their online details.

Banca di Roma (Italy): The phishing site is a replica of the legitimate bank site. If users try to log on to their account, the information that they enter is sent to a remote host, and users are then redirected to the legitimate Website.

Screenshots:

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=685>

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=684>

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=683>

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=682>

Source: <http://www.websensesecuritylabs.com/>

Transportation and Border Security Sector

12. *October 27, Associated Press* — **United flight lands safely in Japan with radio trouble.** A United Airlines flight from Chicago with 174 people aboard landed safely at an airport in western Japan on Wednesday, October 25, after developing radio trouble, officials said. The Boeing 777 had a radio failure while trying to make a landing approach to Kansai International Airport (near Osaka, about 260 miles southwest of Tokyo), said Hiroshi Yasuragi of Transport Ministry's Kansai Office. The pilot of Flight 877 requested an emergency landing at the airport, which was the plane's destination, and landed safely Wednesday, Yasuragi said. The cause of the problem was under investigation.
Source: http://biz.yahoo.com/ap/061025/apfn_united_emergency_landing.html?.v=1
13. *October 27, ABC News* — **Website lets anyone create fake boarding passes.** A 24-year-old computer security student working on his doctorate at Indiana University in Bloomington has created a Website that allows anyone with an Internet connection and a printer to create and print fake boarding passes for Northwest Airlines flights. The passes look virtually identical to the ones printed from the airline's Website, and are intended to get you past security — but not onto an airplane. By entering your name and plugging in information about the flight — flight number, gate, seat number, departing city, destination, departure, and arrival times and class — the Website generates a boarding pass the program's creator says will get you past security checkpoints, even without ID. Christopher Soghoian, creator of "The Northwest Airlines Boarding Pass Generator," knew he would be opening up a can of worms by writing the program and creating the site, but says it's the only way to show people how deeply flawed airport and airline security are. The Transportation Security Administration (TSA) says that what Soghoian has done is illegal and that using one of these bogus boarding passes would be illegal as well. TSA officials also believe that it would do little to aid anyone looking to do harm to airline passengers.
Source: <http://abcnews.go.com/Technology/story?id=2611432&page=1>
14. *October 27, Associated Press* — **Jet makes emergency landing at Kentucky airport.** A regional jet made an emergency landing at Louisville International Airport Friday, October 27, shortly after it took off from the airport with 46 people aboard, a spokesperson said. Airport spokesperson Trish Burke said the American Airlines Embraer E135 jet had communicated with the airport that it had an "engine out" at 4:30 p.m. CDT. It landed 25 minutes later, Burke said. "Initial reports are that it had a brake problem," Burke said, adding that the aircraft was slightly off the runway.
Source: http://www.usatoday.com/travel/news/2006-10-27-landing_x.htm
15. *October 26, GovExec* — **TSA faces staffing disparities at airports.** The Transportation Security Administration (TSA) needs to create uniform guidelines to address inconsistencies in staffing levels of administrative employees across airports, auditors said in a new report. "TSA's initial staffing actions lacked coherency and resulted in some cases in significant disparities in staffing at airports," the report from the Department of Homeland Security inspector general stated. The report was completed September 26 in response to a summer 2005 request from Rep. John Mica, (R-FL), chairman of the House Transportation and Infrastructure Subcommittee on Aviation. But it was not released publicly until this week. The inspector

general report partly noted a concern: "TSA hired and deployed too many administrative staff at some airports and too few at others," it stated. But TSA is developing a policy, known as the "Hub-Spoke Realignment and Reallocation Plan," that will help "render staffing ratios nationwide more uniform," the IG said. The plan entails classifying major airports as hubs and others as spokes, and centralizing staff at the larger airports. TSA would retain the ability to assign workers as needed to smaller airports. Agency officials told the IG the plan will require 139 additional positions, but cited a lack of funding to make the hires.

Report: http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_06-65_Sep06.pdf

Source: http://www.govexec.com/story_page.cfm?articleid=35353&dcn=to_daysnews

- 16. *October 26, GovExec* — Agency delays deadlines to check air-cargo workers.** The Transportation Security Administration (TSA) has delayed security requirements, criminal background checks, and threat assessments for tens of thousands of workers who handle passenger-airplane cargo, saying the aviation industry is unable to meet previous deadlines. The agency has pushed back several deadlines as required under a rule issued earlier this year. "TSA has concluded that the regulated community will be unable to meet some deadlines in the air-cargo final rule because of the large number of employees and agents subject to the requirements," the agency said in a Federal Register notice Wednesday, October 25. TSA spokesperson Darrin Kayser said that other requirements of the rule still apply, such as multiple security layers, random screening and the "known shipper" program. Under the cargo rule, aircraft operators, foreign carriers and indirect air carriers would have until December 1 to ensure that security threat assessments are completed on workers with unescorted access to cargo. The deadline has now been extended until March 15 for employees of aircraft operators, foreign air carriers and indirect air carriers, and June 15 for employees of agents. Kayser said the deadline applies to about 50,000 workers.

Source: http://www.govexec.com/story_page.cfm?articleid=35359&dcn=to_daysnews

- 17. *October 25, Department of Homeland Security* — DHS announces investment in next-generation handheld radiological detection equipment.** The Department of Homeland Security's (DHS) Domestic Nuclear Detection Office (DNDO) announced on Wednesday, October 25, \$113 million in competitive awards to enhance the detection of radiological materials at the nation's ports of entry. "These next generation handheld devices will bring an even faster and more reliable means to detecting and identifying radioactive materials at our ports," said Vayl S. Oxford, DNDO director. "They are part of a robust global nuclear detection architecture built for the most consequential threats to the homeland." DNDO anticipates purchasing and deploying roughly 1,000 next generation handheld systems and 200 backpack systems through the Human Portable Radiation Detection Systems program. The portable technology will be used primarily by U.S. Customs and Border Protection officers for secondary screening of cargo to identify and localize radiological material after a primary alarm has been triggered. It is also anticipated that the devices could be used by U.S. Coast Guard officers aboard vessels prior to an arrival at port. There are more than 14,000 handheld devices in use at the nation's ports.

Source: http://www.dhs.gov/xnews/releases/pr_1161798684239.shtm

[[Return to top](#)]

Postal and Shipping Sector

18. *October 28, Associated Press* — **McCalla post office customers, workers tied up by robbers.** Three armed men tied up customers and employees and then robbed the post office in McCalla, AL, Friday morning, October 27. Inspector-in-Charge of the United States Postal Inspection Service Martin Phanco said no one was injured. Phanco said two more men may have been waiting outside the rural post office. He said the robbers stole the cars of two customers. It was unclear what else they may have taken.
Source: <http://www.nbc13.com/news/10181183/detail.html>

[[Return to top](#)]

Agriculture Sector

19. *October 27, Agence France–Presse* — **New tests at British abbatoir where foot and mouth broke in 2001.** Tests have been carried out for foot and mouth disease at a British abbatoir where the devastating 2001 outbreak was first confirmed after a suspect disease was reported in pigs, the environment ministry said. Restrictions were placed on and around Cheale Meats slaughterhouse and farm near Brentwood, east of London, Thursday, October 26, and samples taken from pigs were sent to be analyzed. Initial results were negative for foot and mouth disease and swine vesicular disease, Britain's chief veterinary officer Debby Reynolds said in a statement issued by the Department for Environment, Food and Rural Affairs.
Source: http://news.yahoo.com/s/afp/20061027/hl_afp/farmhealthbritain_061027141116
20. *October 26, U.S. Department of Agriculture* — **Confirmatory avian influenza tests complete on Ohio duck samples.** The U.S. Department of Agriculture (USDA) and Department of Interior (DOI) Thursday, October 26, announced final test results, which confirm that no avian influenza virus was found in samples collected earlier this month from wild Northern pintail ducks in Ohio. The initial rapid screening tests are sensitive and can detect inactive viruses in samples. It is not unexpected to have positive results on an initial test and then to have confirmatory testing reveal that no active virus is present.
The LPAI H5N1 detection list: <http://wildlifedisease.nbj.gov/ai/LPAITable.pdf>
Source: http://www.usda.gov/wps/portal/!ut/p/s.7_0_A/7_0_1OB/.cmd/a/d/ar/sa.retrievecontent/c/6_2_1UH/.ce/7_2_5JM/.p/5_2_4TQ/.d/1/th/J_2_9D/s.7_0_A/7_0_1OB?PC_7_2_5JM_contentid=2006%2F10%2F0429.xml&PC_7_2_5JM_parentnav=LATEST_RELEASES&PC_7_2_5JM_navid=NEWS_RELEASE#7_2_5JM
21. *October 26, Sports Network* — **More than 1,000 horses quarantined at Monmouth.** The New Jersey Department of Agriculture quarantined more than 1,000 horses at Monmouth Park in Oceanport, NJ, due to a strain of the equine herpes virus. The department confirmed positive test results on at least one horse for the neuropathogenic strain of equine herpes. The equine herpes virus can spread quickly and cause respiratory problems, especially in young horses and result in spontaneous abortions in pregnant mares. The neurologic form of the virus can reach high morbidity and mortality rates.
Information on Equine Herpes: http://www.merckvetmanual.com/mvm/index.jsp?cfile=htm/bc/121_302.htm
Source: <http://seattlepi.nwsourc.com/scorecard/othernews.asp?articleID=177758>

22. *October 26, Reuters* — **More toxic E. coli samples found on California ranch.** Six new samples of toxic E. coli bacteria matching the strain in tainted spinach that killed three Americans and sickened 200 have been found on a California ranch, a state health official said on Thursday, October 26. Investigators have now discovered a total of nine samples of the matching E. coli 0157:H7 strain on the ranch where the spinach was raised, Kevin Reilly, a deputy director with the California Department of Health Services, said. The ranch is in the area of Monterey and San Benito counties, among California's most productive agricultural regions and top producers of fresh, bagged spinach. Investigators have focused on four undisclosed ranches in the area as potential sources of the tainted raw spinach responsible for an E. coli outbreak across 26 U.S. states and one Canadian province. Four of the new matching samples have been traced to cattle on the same ranch and the other two new matching samples were traced to a creek and a wild pig killed on the property, Reilly said.

Source: http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyID=2006-10-26T222246Z_01_N26243070_RTRUKOC_0_US-SPINACH.xml&WTmodLoc=NewsHome-C3-domesticNews-3

[[Return to top](#)]

Food Sector

23. *October 29, Agence France-Presse* — **South Korea to resume U.S. beef imports.** South Korea is to resume imports of U.S. beef ending a ban imposed nearly three years ago over mad cow disease. Nine tons of beef from a Kansas-based slaughterhouse will arrive at Incheon International Airport on Monday, October 30, and will go on sale after detailed quarantine inspections, Yonhap news agency said, quoting government officials on Sunday, October 29. South Korea in January agreed partially to lift the ban imposed in December 2003, but the resumption stalled after the discovery of a new U.S. mad cow case in March.
- Source: http://news.yahoo.com/s/afp/20061029/hl_afp/skoreahealthmadcow_061029150851
24. *October 26, Animal and Plant Health Inspection Service* — **USDA adopts final rule adding Namibia to the list of regions considered free of foot-and-mouth disease.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service is amending its import regulations regarding live swine, certain pork and pork products to add Namibia, except for the region north of the Veterinary Cordon Fence, to the list of regions considered free of foot and mouth disease (FMD) and added the entire country to the list of regions free of rinderpest. Namibia will still be subject to certain import restrictions for FMD and rinderpest, however, because of its proximity to or trading relationships with regions that are not free of these diseases.
- Source: <http://www.aphis.usda.gov/newsroom/content/2006/10/namibfmd.shtml>
25. *October 25, U.S. Food and Drug Administration* — **Ballard's Farm Sausage, Inc. announces an extension of its voluntary recall.** Ballard's Farm Sausage, Inc. announces an extension of its voluntary recall involving all lots of Ballard's Farm 24 ounce Amish Macaroni salad, Ballard's Farm 24 ounce Amish Sweet Slaw, Ballard's Farm 12 ounce Cole Slaw, and Food City 12 ounce Cole Slaw because of a possible health risk. This is in addition to the recall of Ballard's Farm 12 ounce Egg Salad on October 18. Ballard's Farm is announcing this recall

extension based on laboratory tests that show the products may be contaminated with *Listeria monocytogenes*. This organism can cause serious and sometimes fatal infections in young children, frail or elderly people and others with weakened immune systems. Although healthy individuals may suffer only short-term symptoms such as high fever, severe headache, stiffness, nausea, abdominal pain and diarrhea, *Listeria* infection can cause miscarriages and stillbirths among pregnant women.

Source: http://www.fda.gov/oc/po/firmrecalls/ballard210_06.html

[[Return to top](#)]

Water Sector

26. *October 29, Charlotte Observer (NC)* — **Durham water instructions barred.** Federal regulators have issued a nationwide advisory on how to properly screen for lead in drinking water after learning Durham, NC, was instructing homeowners to remove aerators from their faucets before drawing samples. Removing the aerator prior to testing could remove trapped lead particles. On October 20 letter, the U.S. Environmental Protection Agency's director for drinking water protection, Stephen Heare, barred the practice, which Durham has done since it began the mandated tests for lead in 1991.

Source: <http://www.charlotte.com/mld/observer/news/local/15877179.htm>

[[Return to top](#)]

Public Health Sector

27. *October 29, Cleveland Plain Dealer (OH)* — **Veterans hospitals screening for staph.** Veterans hospitals have launched a strategic war against drug-resistant staph bacteria, targeting patients who may unknowingly harbor the bug. The Veterans Administration (VA) says it has found success from a program that screens patients at admission and isolates those who carry the bacteria. The initiative, which began as a small pilot program, is expanding to more patients and more hospitals. So-called "search and isolate" programs are aimed at stopping the rapid spread of methicillin-resistant *Staphylococcus aureus* (MRSA). The VA is adopting the program at 17 hospitals, following its success at the Pittsburgh, PA, VA. The Pittsburgh hospital cut infections by more than 70 percent in surgical units, where infection risks are high, said Robert Muder, chief of infectious diseases. The VA may roll out the procedures nationally, he said.

MRSA information: http://www.cdc.gov/ncidod/dhqp/ar_mrsa.html

Source: <http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/1162114849152530.xml&coll=2>

28. *October 28, Hindu (India)* — **New polio cases reported in India.** Fresh cases of polio have been reported in India. "In the past one week, 21 polio more cases have been confirmed of which 19 are from Uttar Pradesh alone. The total polio cases has now reached 437 in the country," an official of the National Polio Program, said. Uttar Pradesh has reported the maximum number of polio cases, with 377 children being affected with the virus. It is followed by Bihar where 28 cases have surfaced. One fresh case each has been reported from Uttaranchal

and Punjab. Last week, 30 cases were reported, out of which 21 were from Uttar Pradesh alone. Delhi has four polio cases since January this year. Last year, 66 polio cases were reported in India.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: <http://www.hindu.com/thehindu/holnus/002200610282222.htm>

29. *October 27, Reuters* — **Emergency care should use trauma as example.** Most U.S. hospital emergency rooms are ill-equipped to handle an epidemic, but better coordination and sharing specialist doctors could help mend the tattered system, experts said on Friday, October 27. A model for emergency care for the 5,000 overwhelmed emergency rooms exists: the 1,000 designated U.S. trauma centers that meet guidelines for the number and types of surgeons present, equipment and training, doctors said. Trauma centers, specialized units to handle the seriously injured, can coordinate care when an average of one ambulance per minute is sent away from one overtaxed hospital emergency room and diverted to another. Doctors gathered to discuss a series of reports by the U.S. Institute of Medicine, whose major findings were: that ERs are understaffed, overwhelmed and not prepared for a crisis. One idea is to have regional specialists on call to spread their expertise across a greater geographic area.

Source: <http://today.reuters.co.uk/news/articlenews.aspx?type=health>

[News&storyID=2006-10-27T191850Z_01_N27171328_RTRIDST_0_HEALTH-EMERGENCY-DC.XML&WTmodLoc=NewsLanding-C9-SciHealth-3](http://today.reuters.co.uk/news/articlenews.aspx?type=health&News&storyID=2006-10-27T191850Z_01_N27171328_RTRIDST_0_HEALTH-EMERGENCY-DC.XML&WTmodLoc=NewsLanding-C9-SciHealth-3)

30. *October 27, Agence France-Presse* — **World Health Organization hints at treatment priorities in a flu pandemic.** Emergency services, health workers and their relatives should be the first to be protected through medical means if a global flu pandemic breaks out, a senior World Health Organization (WHO) official said. David Heymann, the WHO's special representative on pandemic influenza, made the comments after a meeting this week of experts on ethics and pandemic influenza to discuss issues such as quarantines. With the likelihood of a sudden and rapid spread of a more virulent strain of flu in a pandemic, no immediate prospect of vaccination, and limited supplies of antiviral drugs to reduce the impact of the symptoms, the health community has to confront issues such as whom to treat first, WHO officials said. Police and fire services "and others that are required to maintain order within society" should also be protected, he added. Scientists fear the H5N1 strain of avian influenza, which has caused more than 150 human deaths since 2003, could be a precursor to a global flu pandemic with a potential death toll of millions.

Source: http://news.yahoo.com/s/afp/20061027/hl_afp/whohealthflupandemic_061027184916

[[Return to top](#)]

Government Sector

31. *October 27, Associated Press* — **Powder investigated at Clinton office was harmless.** New York City Police and Secret Service agents are saying there's no cause for alarm about a white powdery substance found at former President Bill Clinton's office in Harlem. A Secret Service spokesperson said officials field tested the powder Friday night, October 27, and found it was harmless. Clinton wasn't at the office at the time. Police said a woman who worked in the building opened an envelope that contained a white powder. Police emergency services officers were called to the Harlem office building at about 3:45 p.m. EDT.

Source: <http://www.nbc6.net/news/10177612/detail.html>

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

Emergency Services Sector

32. *October 26, GovExec* — **Academic urges government-run emergency communications network.** A Carnegie Mellon University expert on Thursday, October 26, called for the development of a government-run communications network that would enable police, firefighters and other emergency responders from different jurisdictions to talk to each other. "A government system is feasible, and it would clearly be more cost effective than what we have today," Jon Peha, an engineering and public policy professor, said during the presentation of a paper on the issue at a forum sponsored by the New America Foundation. Peha said that after the disastrous communications failures on September 11, 2001, and during Hurricane Katrina, he could "not see why we should tolerate" the current decentralized emergency-response system, which gives the flexibility of local "first responder" agencies precedence over standardization and regional cooperation. Peha said a good starting place for a new system would be the congressionally mandated program to double the emergency broadcast bandwidth by reallocating 24 megahertz of prime spectrum from television to public safety as a part of the transition from analog to digital signals in 2009.

Source: http://www.govexec.com/story_page.cfm?articleid=35360&dcn=to_daysnews

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

Information Technology and Telecommunications Sector

33. *October 27, Security Focus* — **Microsoft .NET framework request filtering bypass vulnerability.** Microsoft .NET framework is prone to a vulnerability that may permit the bypassing of content filtering. An attacker can exploit this issue to perform multiple input validation attacks such as cross-site scripting, SQL-injection, and HTML-injection; other attacks are also possible. Vulnerable: Microsoft .NET Framework 2.0. Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.
Source: <http://www.securityfocus.com/bid/20753/references>
34. *October 27, Associated Press* — **Sony battery emits sparks during recall.** A Sony-made battery used in a Fujitsu laptop computer overheated and emitted sparks, Fujitsu said Friday, October 27, amid a massive global recall involving Sony batteries. A Fujitsu worker was visiting a customer's home to retrieve the laptop as part of the company's recall of Sony batteries when it overheated and started giving off sparks, according to Fujitsu spokesperson Toshiaki Koike. No one was injured in the incident, which is under investigation, Koike said.
Source: http://news.yahoo.com/s/ap/20061027/ap_on_hi_te/japan_battery_recall
35. *October 27, VNUNet* — **Security vendor circumvents Windows Vista's Patchguard.** Security researchers with Authentium have found a way to circumvent the Patchguard security technology that Microsoft has built into the 64-bit version of its forthcoming Windows Vista operating system. Over the past months the Patchguard technology has been subject of a fierce

debate between security vendors and Microsoft because it prevents some anti-virus software from functioning. Authentium's technology allows an application to effectively disable Patchguard. In a blog posting the company argued that providing kernel access to third party Websites will enable future security innovations.

Source: <http://www.vnunet.com/vnunet/news/2167387/security-vendor-circumvents>

- 36. *October 27, Sophos* — Company which sent over 200 million spam messages fined \$4.1 million.** An Australian company and its director have been fined a total of \$4.1 million after it was claimed they sent over 200 million spam e-mails in a 12 month period. The Perth, Western Australia-based spammer, Wayne Mansfield, and his company Clarity1, were found to have illegally sent out millions of spam messages in the 12 months since Australian spam laws were introduced in April 2004. In April 2005, Sophos reported how authorities in Australia raided a suspected spam factory in Perth, during which the contents of computer hard disks and other material were seized. "This is the first time that spammers have been successfully prosecuted under the Australian Spam Act, and represents a victory for the authorities and the man in the street pestered by nuisance e-mail," said Graham Cluley, senior technology consultant for Sophos.

Source: <http://www.sophos.com/pressoffice/news/articles/2006/10/clarity-spam.html>

- 37. *October 26, CNET News* — Linux guru warns on security of open-source code.** Alan Cox, one of the most respected figures in the UK open-source community, has warned about complacency over the security of open-source projects. Speaking to delegates at London's LinuxWorld conference on Wednesday, October 25, he emphasized that considerable sums of money were being spent in attempting to hack into open-source systems. And he cautioned that many open-source projects were far from secure. "Things appear in the media, like 'open-source software is more secure, more reliable and there are less bugs.' Those are very dangerous statements," Cox said. Cox said that analysis looks only at well-known projects. An analysis of 150 projects from SourceForge, a repository for open-source code, would not result in the same high marks that the Linux kernel would get, he noted. "High-quality only applies to some projects — those with good code review and those with good authors," Cox said.

Source: http://news.com.com/Linux+guru+warns+on+security+of+open-source+code/2100-1002_3-6129835.html?tag=ne.fd.mnbc

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	25 (smtp), 1026 (win-rpc), 1434 (ms-sql-m), 53 (domain), 139 (netbios-ssn), 1027 (icq), 445 (microsoft-ds), 135 (epmap), 1433 (ms-sql-s), 80 (www)
Source: http://isc.incidents.org/top10.html ; Internet Storm Center	
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/ .	

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[[Return to top](#)]

General Sector

38. *October 29, Associated Press* — Blaze that killed firefighters is 70% contained. Firefighters aided by dying winds on Sunday, October 29, appeared to be winning the battle against a 63-square-mile wildfire that killed four of their own and destroyed 34 homes. The fire was set shortly after 1 a.m. Thursday at the base of a slope in the desert city of Cabazon, about 10 miles northwest of Palm Springs. The 40,450-acre blaze, which authorities say was set by an arsonist, was 70 percent contained. The blaze was still threatening a wilderness area plagued by drought and filled with dead trees, but fire officials were confident that if they could keep it out of that area they could have it under control by Tuesday night. As firefighters were getting the upper hand on that blaze another broke out Sunday in Warner Springs, a rural community about 70 miles northeast of San Diego. That fire began about noon and quickly blackened about 100 acres, forcing the evacuation of several homes, said Capt. David Janssen of the California Department of Forestry. More than 200 firefighters, five helicopters and an air tanker rushed to the scene to defend about 14 homes in the blaze's path. The cause was under investigation. Source: http://www.latimes.com/news/local/la-102906fire_wr.0.6719042.story?coll=la-home-headlines

[[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.