



# Department of Homeland Security Daily Open Source Infrastructure Report for 24 August 2007

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

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

## Daily Highlights

- ComputerWorld reports California Public Employees' Retirement System officials are sending letters of apology to about 445,000 state retirees after inadvertently printing their Social Security numbers on brochures announcing an upcoming election at the state pension fund. (See item [13](#))
- The New York Times reports the five levees that protect the metropolitan area of East St. Louis, Illinois, from the Mississippi River do not meet the Federal Emergency Management Agency's standards for flood protection and will be removed from maps that record flood vulnerability. (See item [38](#))

### DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

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

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *August 23, Platts Energy Bulletin* — **AEP and Allegheny finalize deal to build high-voltage power line.** American Electric Power (AEP) and Allegheny Energy on Thursday, August 23, said they have finalized a joint venture they announced in April to build a 290-mile, high-voltage transmission line from West Virginia to Maryland. The companies' Potomac-Appalachian Transmission Highline project includes approximately 244 miles of 765 kV extra-high voltage transmission from AEP's Amos substation near St. Albans, WV, to the

Bedington substation, northeast of Martinsburg, WV. Another 46 miles of transmission, consisting of twin-circuit 500 kV transmission, will be built from Bedington to a new substation at Kempton, southeast of Frederick, MD. The total project is estimated to cost approximately \$1.8 billion, with AEP paying approximately \$600 million and Allegheny \$1.2 billion. The PJM Interconnection — a regional transmission organization that ensures the reliability of the electric power supply system in 13 states and the District of Columbia — has said the new line will be needed by 2012 to ensure reliability in the region.

Source: [http://www.platts.com/Electric\\_Power/News/6440294.xml?sub=Electric\\_Power&p=Electric\\_Power/News](http://www.platts.com/Electric_Power/News/6440294.xml?sub=Electric_Power&p=Electric_Power/News)

2. *August 23, Platts Energy Bulletin* — **German government, utilities agree on nuclear safety improvements.** The German environment ministry and the country's four biggest utilities — E.ON, RWE, ENBW and Vattenfall Europe — have agreed to improve safety culture and operations of nuclear power plants in Germany within one year, the environment ministry said Thursday, August 23, in a statement. A debate over safety, information policy and the operation of German nuclear power plants started after Vattenfall Europe's Brunsbuttel and Krummel reactors had to be taken off the grid June 28 in emergency shutdowns after a short circuit at Brunsbuttel and a fire at one of Krummel's transformer stations. According to the statement, key improvements are to include: the operators' safety management systems are to be improved; regular scheduled safety investigations by state authorities are to be intensified and their processing accelerated; protection against gas penetration of the power plants' control rooms is to be improved; internal communication of facilities is to be improved.

Source: <http://www.platts.com/Nuclear/News/8220816.xml?sub=Nuclear&p=Nuclear/News>

3. *August 23, Business Review* — **National Grid approved to acquire KeySpan.** The New York State Public Service Commission unanimously voted to approve National Grid's acquisition of KeySpan on August 22. National Grid is paying \$42 for each share of KeySpan, or \$7.3 billion, resulting in the creation of the third-largest energy-delivery company in the United States. KeySpan is the largest supplier of natural gas in the Northeast, and also transmits electricity on Long Island. National Grid is based in Britain and has its U.S. headquarters in Westborough, MA. KeySpan becomes National Grid's fifth U.S. acquisition. It acquired Niagara Mohawk in 2002. KeySpan becomes a wholly owned subsidiary of National Grid, which says it will maintain KeySpan's Brooklyn office and its own Westborough facility.

Source: <http://biz.yahoo.com/bizj/070823/1510408.html?.v=1>

4. *August 22, Platts Energy Bulletin* — **Kentucky considers offering pre-construction money for clean-coal.** An energy incentive bill, aimed in part at attracting a Peabody Energy clean-coal project to Kentucky, passed its first test Tuesday afternoon, August 21, winning approval by a 26 to two margin by the Appropriations and Revenue Committee of the state House. Instead of the usual method of offering incentives as certain milestones are met, this bill would tempt companies to move their clean-coal projects to Kentucky provided the plans meet certain qualifications. Under the legislation, companies wanting to invest in clean coal or renewable energy projects could receive millions of dollars in up-front cash payments from the state. More companies planning coal-to-liquids and/or coal gasification projects are eyeing the Bluegrass state, according to Kentucky Economic Development Secretary John Hindman.

Source: <http://www.platts.com/Coal/News/6439438.xml?sub=Coal&p=Coal/News>

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

## **Chemical Industry and Hazardous Materials Sector**

5. *August 23, Tennessean* — **Tanker crash prompts road closure.** The tanker truck driver who died Wednesday, August 22, in a fiery crash on Briley Parkway in Nashville, TN's, Bordeaux area remains unidentified as of Thursday, August 23, said Metro police. The wreck happened about 5 p.m. CDT as the driver, who was hauling gasoline, was in the northbound lanes. He drifted to the right, but flipped the truck onto its passenger side when he tried to straighten up. It immediately ignited, sending black smoke billowing into the air. All lanes of Briley Parkway were closed for hours on Wednesday.  
Source: [http://tennessean.com/apps/pbcs.dll/article?AID=/20070823/NE\\_WS03/70823017/1017](http://tennessean.com/apps/pbcs.dll/article?AID=/20070823/NE_WS03/70823017/1017)
  
6. *August 22, NBC 4 (Washington, DC)* — **Collision causes pool chemicals to leak, four hospitalized.** Maryland police are investigating a two-car crash on Route 301 in Upper Marlboro. Officials said that at about 8 a.m. EDT on Wednesday, August 22, a car traveling southbound along Route 301 between Route 4 and Marlboro Pike crossed the median and struck a van carrying pool chemicals. Authorities said that some of the chemical escaped from the containers, creating a vapor cloud. Four people were transported to the hospital as a precaution. The roadway was closed for clean up and investigation.  
Source: <http://www.nbc4.com/news/13947165/detail.html>

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

## **Defense Industrial Base Sector**

7. *August 23, Federal Computer Week* — **Military brass: Acquisition rules can't keep up with IT needs.** Cumbersome acquisition rules designed more for building weapons systems and computing platforms are posing a growing obstacle to rapidly evolving information technology networks, members of a panel of generals said at the LandWarNet conference in Fort Lauderdale, FL, this week. "One of the biggest challenges within the Department of Defense is ourselves and the FAR [Federal Acquisition Rules]," said Brig. Gen. George Allen, director of command, control, communications and computers for the Marine Corps. Allen cited the frustration his organization experienced in Operation Iraqi Freedom 1 in installing the largest communications and data network ever built by the Marines. The project used the latest available technologies "from an acquisition point of view, but which in fact were four years old," he said. "We had to buy new Dell servers and Cisco routers to get the network to work" as intended. "When you're talking switchers and routers, they change every six months," Allen said, but FAR rules don't allow the necessary flexibility to keep networks evolving to meet emerging needs. "We buy IT systems the way we buy aircraft carriers," he said, noting that contracting rules need to be changed for basic technology refreshes.  
Source: <http://www.fcw.com/article103570-08-23-07-Web>
  
8. *August 22, GovExec* — **Watchdog urges Defense agency to better control interagency buys.** Inadequate internal procedures have prevented the Missile Defense Agency from guaranteeing

that purchases made in conjunction with other agencies are in the government's best interest and fully compliant with federal regulations, according to a new report by the Department of Defense inspector general (IG). The IG report found that during the two-year period from March 2004 to March 2006, the Missile Defense Agency repeatedly misused and failed to properly manage both outgoing and incoming Military Interdepartmental Purchase Requests (MIPRs). Such requests are issued by one military service to another service or a civilian federal agency to procure supplies, services or equipment. Auditors examined 47 MIPRs and found that the Missile Defense Agency did not follow standard regulations to ensure that the interagency funds were properly obligated, expensed or disbursed.

IG Report: <http://www.dodig.osd.mil/Audit/reports/FY07/07-117.pdf>

Source: [http://www.govexec.com/story\\_page.cfm?articleid=37835&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=37835&dcn=to%20daysnews)

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

## **Banking and Finance Sector**

9. *August 23, Sophos (UK)* — **AOL identity thief faces seven year jail sentence.** Experts at Sophos have reminded computer users of the threat posed by phishers following the conviction of a 23-year-old identity thief who targeted users of AOL. Michael Dolan, formerly from West Haven, CT, and North Miami Beach, FL, has admitted stealing names, credit card details and social security numbers from AOL members. From 2002 until his arrest on September 26, 2006, Dolan used malicious software to steal AOL screen names from chat rooms. The users were then spammed with electronic greeting cards claiming to be from Hallmark.com, but which in reality installed a Trojan horse that prevented AOL customers from logging into their account without entering personal information. Dolan would use the stolen information to order online goods and steal money from ATM machines. A plea agreement with the U.S. Department of Justice calls for Dolan to spend seven years in prison, and then remain on supervised probation for two to three years. He may also have to pay a fine of \$250,000. Source: <http://www.sophos.com/pressoffice/news/articles/2007/08/dolan.html>

10. *August 23, Sophos (UK)* — **High volume phish campaign strikes Australian Internet users.** Sophos is warning Australian banking consumers not to be duped by a high-volume spam campaign aimed at tricking Westpac customers into "reviewing their account information" online. Sophos reports that the phish e-mail, which arrives with a subject line of "Westpac Internet Bank hardware problems," has shown up exclusively in its Australian spamtraps, but at around ten times the local volume typically seen in less targeted spam campaigns. "Westpac has suffered neither 'recent hardware failure,' nor 'partial loss of information,' as the scammers claim," said Paul Ducklin, Head of Technology, Asia Pacific, at Sophos in Sydney. Sophos reports that the fake Websites linked to this phish are currently off-the-air, which limits the damage that can be done, but urges users not to click through anyway, even in a spirit of research. Source: <http://www.sophos.com/pressoffice/news/articles/2007/08/hardware-phish.html>

11. *August 23, Associated Press* — **Laptop with New York City retirees' data stolen.** A laptop loaded with financial information on as many as 280,000 New York City retirees was stolen from a consultant who took the computer to a restaurant, city officials said. The private consultant to the city Financial Information Services Agency had access to personal data about

members of various city pension systems, mayoral spokesperson Jason Post said Wednesday, August 22. The consultant told authorities Monday the portable computer had been stolen. Post said the city would notify any retirees whose data might be compromised.

Source: [http://webstv.com/newyorkwire/NY--ComputerSecurity/resources\\_news\\_html](http://webstv.com/newyorkwire/NY--ComputerSecurity/resources_news_html)

12. *August 22, ComputerWorld* — **Monster.com Trojan recruits money launderers from victim pool.** The Trojan responsible for stealing more than 1.6 million personal records from Monster.com uses that information to build targeted spam that offers recipients lucrative, but illegal, money laundering jobs, said Symantec Corp. Wednesday, August 22. Monster.com, meanwhile, said Wednesday it had shut down the server used to store the stolen resume information. Earlier this week, Symantec fingered Infostealer.Monstres for using stolen Monster.com log-ons to run automated searches. Criminals then used the stolen information to create convincing e-mail messages that contained malicious code. Some of those messages included Banker.c, a password-stealing Trojan horse that monitored the infected PC for log-ons to online banking accounts. But Monstres is also equipped to recruit criminal collaborators. "What we offer you is something more than just a job — it's the opportunity to earn really big money without having to work much," read one of the messages. Among the job requirements, said the messages, were a new checking account with Bank of America. Although the job offer didn't spell it out in so many words, it's clear that the work involves cleaning out accounts of phishing victims, possibly the very ones hit by the Banker.c Trojan. Source: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032278&intsrc=hm\\_list](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032278&intsrc=hm_list)

13. *August 22, ComputerWorld* — **California state pension fund admits breach of retiree data.** Officials at the California Public Employees' Retirement System (CalPERS) are sending out letters of apology to about 445,000 state retirees after inadvertently printing their Social Security numbers on brochures announcing an upcoming election at the state pension fund. The error happened last week and has already prompted several changes at CalPERS to reduce the chances of something similar happening again, said spokesperson Pat Macht. According to Macht, the privacy breach happened after an employee inadvertently sent a disk containing Social Security numbers to the printer responsible for printing the brochures. Although the printer had an alert system for detecting and preventing the inadvertent publication of Social Security numbers, Macht said, many of the numbers that wound up being printed on the address panels of the brochures began with a series of zeros. That may have confused the system into thinking the figures were member numbers or some other sort of identifier, she said. Source: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032159&intsrc=hm\\_list](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032159&intsrc=hm_list)

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

## **Transportation and Border Security Sector**

14. *August 23, Associated Press* — **U.S. airlines expect Labor Day increase.** Despite record-level delays, nearly 16 million passengers will fly on U.S. airlines over the Labor Day weekend, a 2.6 percent increase over a year ago, estimates an industry group. The Air Transport Association on Thursday, August 23, forecast 15.7 million passengers will travel globally on U.S. airlines between August 29 and September 5. The group, which represents AMR Corp.'s

American Airlines, UAL Corp.'s United Airlines, and others, said while most delays would be weather related, a modernized air traffic control system is needed to reduce air traffic congestion. The airlines and the Federal Aviation Administration are pushing Congress to authorize financing of a multibillion-dollar upgrade of the air traffic control system.

Source: [http://biz.yahoo.com/ap/070823/airlines\\_labor\\_day.html?.v=1](http://biz.yahoo.com/ap/070823/airlines_labor_day.html?.v=1)

15. *August 23, Jacksonville Business Journal* — **JIA's preferred traveler program extended to 10 airports.** People flying in and out of Florida's Jacksonville International Airport (JIA) can now use JIA's preferred traveler program at 10 other airports in the U.S. The program is an enhanced version of the Transportation Security Administration's registered traveler program, which will provide expedited security screening for airline passengers. At its most basic level, the program allows passengers to use the shorter security line that airline and airport personnel use. They and their bags must be screened like other passengers. The basic membership, called the silver level and costing \$150 a year, only provides access to the designated security lane. The gold level, at \$250 a year, adds nonstop access in and out of hourly and daily parking garages with automatic billing to a credit card account. The highest level, platinum, costs \$350 a year and includes basic privileges plus the parking benefits and access to the VIP lounge. Members in the program must provide biometric data — fingerprints and an iris scan — that will be stored digitally on a smart card.

Source: [http://jacksonville.bizjournals.com/jacksonville/stories/2007/08/20/daily23.html?jst=b\\_in\\_hl](http://jacksonville.bizjournals.com/jacksonville/stories/2007/08/20/daily23.html?jst=b_in_hl)

16. *August 22, Daily Bulletin (CA)* — **Medical device triggers Los Angeles/Ontario International Airport alert.** A suspicious package prompted the evacuation of a terminal at Los Angeles/Ontario International Airport for more than two hours Wednesday afternoon, August 22. The evacuation and flight delays at the terminal started about noon after officials found what was later determined to be an oxygen medical device during a luggage screening, airport spokesperson Maria Fermin-Tesoro said. The Ontario Fire Department, Ontario Airport Fire Department, the FBI's bomb squad, the Ontario Police Department, the Ontario Airport Police Department, and the Transportation Security Administration assisted with the investigation. Ontario Airport Police K9 units also inspected the inside of the terminal, Tesoro-Fermin said.

Source: [http://www.dailybulletin.com/news/ci\\_6694354](http://www.dailybulletin.com/news/ci_6694354)

17. *August 21, East Valley/Scottsdale Tribune (AZ)* — **Sky Harbor adds black lights, magnifying glasses to security.** The person checking boarding passes and driver's licenses at a Phoenix Sky Harbor International Airport checkpoint is now a trained Transportation Security Administration (TSA) inspector. Armed with magnifying glasses to spot doctored IDs and black lights to examine holograms on driver's licenses or passports, the inspectors are looking for suspicious boarding pass holders. Until a few months ago, airline contract workers were gatekeepers at the security checkpoints, said Nico Melendez, TSA spokesperson. The government watchdogs decided to pilot a program in Phoenix to fill the jobs with their own inspectors, Melendez said. He said the pilot program has been deemed a success, and the TSA is rolling it out nationwide, filling 1,300 checkpoint entry slots in airports around the country. The trained inspectors are better at spotting phony documents, he said, and they get an updated government watch list before every shift. The TSA workers have turned several would-be Sky Harbor passengers with faux IDs over to airport law enforcement officers, Melendez said.

Source: [http://license.icopyright.net/user/viewFreeUse.act?fuid=NDEz\\_OTAx](http://license.icopyright.net/user/viewFreeUse.act?fuid=NDEz_OTAx)

18. *August 18, Baltimore Sun* — **Virginia man arrested at BWI with gun.** A Virginia man who appeared to be "exhibiting suspicious behaviors" was arrested at Baltimore–Washington International Thurgood Marshall Airport (BWI) this month while carrying a concealed handgun with 30 rounds of ammunition, according to the federal Transportation Security Administration (TSA). The August 1 incident was not publicly announced at the time, but an account was later posted on the TSA Website as an example of the success of its technique of screening passengers by closely observing their behavior. The program has been in place at BWI for almost a year. The man told officers that he intended to get a permit for the weapon but had not gotten around to it. The TSA said a behavior–detection officer at the airport observed a man who aroused his suspicions as the passenger stood at an airline ticket counter.

Source: <http://www.baltimoresun.com/news/local/bal-md.bwi18aug18.0.5.400373.story>

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

## **Postal and Shipping Sector**

19. *August 22, North Jersey Media Group* — **Pequannock, New Jersey, police get suspicious package.** The township municipal complex was evacuated this afternoon after the police chief opened a suspicious letter containing an unknown substance that authorities said could have been anthrax. Preliminary tests later determined that they were likely glass beads, authorities said. Police Chief Brian Spring opened an envelope that contained what Morris County Prosecutor Robert A. Bianchi described as "a number of honey–colored BB–like pellets" around 1:45 p.m. The police headquarters is connected to Town Hall. "The first word of the letter was anthrax," said Lt. Dan Dooley, noting the letter was addressed to the detective bureau. Preliminary tests determined that the contents were neither hazardous nor biological in nature, said Bianchi, the prosecutor. Bianchi said that the substance would be sent to the state Department of Health and Senior Services for further testing.

Source: <http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVFeXk1MTkmZmdiZWw3Zjd2cWVIRUV5eTcxODUwMzYmeXJpcnk3ZjcxN2Y3dnFIZUVFeXkz>

20. *August 22, Pueblo Chieftain (CO)* — **Suspicious powder locks down Estes plant in Colorado.** A white powdery substance sent two people to the hospital and caused a possible hazardous materials scare at the Estes–Cox Corp. model rocket plant Tuesday, August 21. Penrose Volunteer Fire Department Assistant Chief Calvin Sundermann said his crew was dispatched shortly after 3 p.m. on a report of a possible hazardous materials situation at the model rocket plant. "A shipment of rocket parts from China had a white powdery substance on a box," Sundermann said. "Two male employees who had the most exposure because they were unloading the truck felt ill and as a precaution were taken to the hospital." Those two employees were treated and released from St. Thomas More Hospital in Canon City, according to hospital spokesperson Jennifer Kemp.

Source: <http://www.chieftain.com/metro/1187816848/18>

21. *August 21, Reuters* — **New York City powder investigation.** New York police said on

Tuesday, August 21, they were investigating suspicious mailings of white powdery substances received by several financial companies in the New York City, a police spokesperson said. "None of the material tested so far has tested positive for any dangerous substance, and was found in some instances to be flour or corn starch," said police spokesperson Paul Browne. He said envelopes containing Zip-lock bags with the powder inside and greeting cards without a message and postmarked from Hartford, CT, were sent to the companies on Monday and Tuesday. He did not name the companies that received the mailings.

Source: <http://www.cnbc.com/id/20379368>

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

## **Agriculture Sector**

### **22. *August 23, Agricultural Research Service* — Genetic GPS for tracking boll weevils.**

Fortunately, the boll weevil (*Anthonomus grandis*), which devastated U.S. cotton crops for much of the 20th century, is now found only in parts of the mid-South and South Texas, thanks to eradication efforts. But monitoring weevils to keep track of where they are coming from — and where they're going — is vital for protecting cotton crops in the U.S. Agricultural Research Service (ARS) entomologist Tom Sappington works in the ARS Corn Insects and Crop Genetics Research Unit at Ames, IA. He has tracked local weevil movements by marking the insects with enamel paint or fluorescent powders and recapturing them later. Now he uses "microsatellites" — short, repetitive DNA sequences — and population assignment tests to find out where weevils in different populations have come from. These tests help pinpoint the migratory patterns and origins of boll weevils over long distances. Sappington's work demonstrates that powerful microsatellite markers and population assignment tests are practical tools for identifying the origins of boll weevils found in areas that have previously been weevil-free. In addition, identifying boll weevil migrants within established weevil populations and knowing where these new migrants came from will foster better strategies for monitoring and managing boll weevil pest introductions.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

### **23. *August 22, Agence France-Presse* — Carcinogens discovered on Belgian farms.** Excessive amounts of cancer-causing substances have been found among cattle on a farm in Flanders, prompting health authorities to test neighboring farms, the Belgian authorities said Wednesday, August 22. The traces of dioxins and PCBs (polychlorinated biphenyls) were found during tests last week at the farm in Statbroek, north of Antwerp near the Dutch border, the federal food safety agency AFSCA said in a statement. Tests at four neighboring farms revealed that two of them also had levels of dioxins and PCBs that slightly exceeded norms, AFSCA said. AFSCA could not pinpoint the origins of the contamination, but it recalled that dioxins and PCBs had been used extensively in the 1970s to manufacture electrical transformers.

Source: <http://www.france24.com/france24Public/en/administration/afp-news.html?id=070822195452.0q8gkjse>

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

## **Food Sector**

24. *August 23, Economic Times (India)* — **China to launch new label on food exports.** China will next month begin marking food exports that pass quality tests with a special label, following recent safety scandals that have hurt the industry's reputation, state media said Thursday, August 23. Food exports that have passed inspections will carry the label "CIQ", which stands for China Inspection and Quarantine, the China Daily reported, citing a regulation from the nation's quality watchdog. Packing must also carry information, such as the producer's name and address, batch number and production date, to keep the source of any potential quality problems on record and stem fake exports, the report said. The new labeling system would begin on September 1.

Source: [http://economictimes.indiatimes.com/News/News\\_By\\_Industry/Cons\\_Products/China\\_to\\_launch\\_new\\_label\\_on\\_food\\_exports/articleshow/2302728.cms](http://economictimes.indiatimes.com/News/News_By_Industry/Cons_Products/China_to_launch_new_label_on_food_exports/articleshow/2302728.cms)

25. *August 23, Associated Press* — **Poisonous puffer fish sold as salmon.** A doctor in Thailand says unscrupulous vendors have been selling meat from the highly poisonous puffer fish disguised as salmon. That's resulted in the deaths of more than 15 people over the past three years. Some 115 people have been hospitalized. The ovaries, liver and intestines of the puffer fish contain a poison so potent that the U.S. Food and Drug Administration says it can "produce rapid and violent death."

Source: <http://www.foxnews.com/story/0,2933,294190,00.html>

26. *August 21, Rutgers* — **Natural food and plant based bioactives offer alternative strategies for food safety.** Chemists and food scientists at Rutgers joined forces to develop natural approaches to the prevention of food contamination and spoilage. The researchers employed natural antimicrobial agents derived from sources such as cloves, oregano, thyme and paprika to create biodegradable polymers or plastics to potentially block the formation of bacterial biofilms on food surfaces and packaging. Typically, a variety of bacteria will congregate on a surface to form a bacterial community that exists as a slime-like matrix referred to as a biofilm. This kind of bacterial community is often described as being polymicrobial; it harbors multiple versions of infectious, disease-causing bacteria. "We mated natural substances with controlled-release, biodegradable polymers that could inhibit or prevent the formation of bacterial biofilms," explained Ashley Carbone, a graduate student at Rutgers who constructed the polymer compounds that were tested.

Source: <http://ur.rutgers.edu/medrel/viewArticle.html?ArticleID=5918>

27. *August 21, ABC (Australia)* — **South Korea expected to resume U.S. beef imports.** U.S. agriculture officials expect South Korea to resume imports of American beef this week, almost a month after they were suspended when a U.S. abattoir sent prohibited bone-in beef to Korea. But U.S. Department of Agriculture deputy under secretary Chuck Lambert says the Koreans will impose new conditions including tougher U.S. inspection safeguards, after the third U.S. shipment this year contained prohibited bone-in beef. "We are taking additional measures and have agreed that any plant that gets suspended for shipping bone-in product will stay suspended until the new protocol is negotiated and in place," he said.

Source: <http://www.abc.net.au/rural/news/content/2007/s2011036.htm>

[[Return to top](#)]

## Water Sector

28. *August 22, Dallas Morning News* — **State-of-the-art system aids new utility operations center.** After the September 11, 2001, terrorist attacks, Garland, TX, conducted a vulnerability study and found that many people could access the former Water Operations Center. The new building, which opened its doors July 30, is a long leap from the Water Operations Center's north Garland home of 60-plus years. Because no building plans were turned in while the site was constructed, Jack May, the city's managing director of water, wastewater and facilities said, no one can access the plans. The fiber-optic part of the security camera system cost is hack-proof, May said. Fiber optics also allow for more security cameras, which keep watch over the city's tanks and manholes. Seven water systems operators monitor the 18 cameras all day, every day. There is a Global Positioning System chip in each water operations vehicle. Each truck comes equipped with a Toughbook laptop. Water systems operators upload work orders to each vehicle and can track which vehicle is closest to the work that needs to be completed.

Source: <http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/DN-garfocust23eas.ART0.North.Edition1.423bdf.html>

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

## Public Health Sector

29. *August 23, World Health Organization* — **International spread of disease threatens public health security.** More than at any previous time in history, global public health security depends on international cooperation and the willingness of all countries to act effectively in tackling new and emerging threats. That is the clear message of this year's World health report entitled *A safer future: global public health security in the 21st century*, which concludes with six key recommendations to secure the highest level of global public health security: full implementation of the revised International Health Regulations (IHR 2005) by all countries; global cooperation in surveillance and outbreak alert and response; open sharing of knowledge, technologies and materials, including viruses and other laboratory samples, necessary to optimize secure global public health; global responsibility for capacity building within the public health infrastructure of all countries; cross-sector collaboration within governments; and increased global and national resources for training, surveillance, laboratory capacity, response networks, and prevention campaigns.

World Health Report: [http://www.who.int/entity/whr/2007/whr07\\_en.pdf](http://www.who.int/entity/whr/2007/whr07_en.pdf)

Source: <http://www.who.int/mediacentre/news/releases/2007/pr44/en/in dex.html>

30. *August 22, Channel NewsAsia* — **Singapore sets up bird flu control system in Indonesia.** Singapore has established a bird flu control system for its bird flu pilot project in Indonesia's Tangerang city. Charun Sopandi, head of the husbandry division at Tangerang's municipal agriculture and husbandry office, said two volunteers would be stationed at each of the more than 100 villages. They would get first-hand information on suspected bird flu sufferers, and would then inform the city administration and the central government of suspected bird flu cases for quick treatment.

Source: <http://www.channelnewsasia.com/stories/singaporelocalnews/vi>

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

## **Government Sector**

Nothing to report.

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

## **Emergency Services Sector**

### **31. *August 22, Hometown Annapolis (MD)* — Bridge crash in Maryland reveals radio troubles.**

State agencies in Maryland couldn't communicate with each other or with Anne Arundel and Queen Anne's counties' emergency units that were first to respond to a fatal Bay Bridge accident on May 10, according to a state report disputed by local officials. The final report on the accident isn't complete. It's expected to include the official cause of the accident and any potential charges. Officials with the Maryland Transportation Authority Police couldn't say when the final report would be released. Part of the internal review of how crews responded to the seven-vehicle accident, which killed three people when a small luggage trailer detached from an SUV heading westbound on the bridge, found that participating agencies couldn't directly communicate with each other. "All communications were either relayed between officers on the scene to communications centers, then to the desired recipient; or were relayed person to person at the scene, and then relayed to the desired recipient," according to an excerpt of the internal review.

Source: [http://www.hometownannapolis.com/cgi-bin/read/2007/08\\_22-46/TOP](http://www.hometownannapolis.com/cgi-bin/read/2007/08_22-46/TOP)

**32. *August 22, Federal Emergency Management Agency* — FEMA was poised and ready for Tropical Storm Erin in Texas.** The Department of Homeland Security's Federal Emergency Management Agency (FEMA) was prepared and ready for Tropical Storm Erin as it made landfall on the Texas coast on August 16. As Erin swirled in the Gulf of Mexico, the Regional Response Coordination Center in Denton was activated to monitor the storm. An advance team consisting of FEMA analysis and leadership officials was sent to Corpus Christi. This group was accompanied by a support team from the Defense Coordinating Element (DCE), a facility capable of providing resources from the U.S. military as needed following a disaster. The DCE team arrived with vehicles equipped with the most advanced technology for transmitting video signals, satellite phone communications and Internet capability. These vehicles are used to provide information to the Region VI office and FEMA Headquarters in Washington, DC. With this up to date information, FEMA specialists away from the coastal area can analyze data and make assumptions about future requests from the state for emergency assistance. In advance of the storm, FEMA positioned emergency commodities such as water, MREs, cots and blankets in Austin. Luckily, these supplies were not needed in Texas for Erin.

Source: <http://www.fema.gov/news/newsrelease.fema?id=39050>

**33. *August 22, Government Technology* — Akron, Ohio, and Summit County collaborate on cellular 911 service.** Summit County, OH, and the City of Akron are reinforcing an ongoing

collaborative relationship, by partnering on a new 911 emergency phone system. As of this week, 911 operators now have the technical capability of pinpointing the locations of emergency calls made from cell phones. This City–County partnership led to the collective purchase of a single 911 emergency phone system to serve both. The agreement will also ensure maintenance expenses will be reduced by as much as 40 percent by eliminating redundancies. With this purchase, the new 911 system now goes above and beyond the previous technology to keep up with the abundance of cellular devices. City and county call takers in the 911 dispatch center will now be provided with telephone numbers and locations for wireless 911 calls as well as for so–called traditional, land–line phones. The new system will automatically display a caller's location on a map at the call taker's station after receiving positioning information from the wireless phone. This will give the call taker the location of the caller. Previously there was no such information available from a cellular call to 911.

Source: <http://www.govtech.com/gt/articles/132372>

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

## **Information Technology and Telecommunications Sector**

**34. August 22, eWeek — Trend Micro fixes security flaws.** Trend Micro has patched several vulnerabilities in its ServerProtect, Anti–Spyware and PC–cillin products that could be exploited remotely to allow hackers to execute arbitrary code. Several vulnerabilities affected ServerProtect, which provides anti–virus protection for Microsoft Windows and Novell NetWare servers. According to researchers at iDefense Labs, in Sterling, VA, an integer overflow exists within the RPCFN\_SYNC\_TASK function, which allocates memory based on a user–supplied integer within the request data. A number of boundary errors can be used to trigger buffer heap and/or stack–based buffer overflows. All of the vulnerabilities affect ServerProtect for Windows 5.58 Build 1176 (Security Patch 3), iDefense officials said, adding that previous versions and versions for other platforms are suspected to be vulnerable as well. The company has released Security Patch 4 to plug the security gaps. In addition, Trend Micro recently fixed flaws affecting version 3.5 of its Anti–Spyware offering, as well as PC–cillin Internet Security 2007.

Trend Micro Patches: <http://www.trendmicro.com/download/product.asp?productid=17>

Trend Micro Hotfix: <http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1035845>

Source: <http://www.eweek.com/article2/0.1895.2174124.00.asp>

**35. August 22, IDG News Service — IBM buys Web conferencing vendor WebDialogs.** IBM has acquired a Web conferencing service provider, it announced as part of a flurry of unified communications moves on Wednesday, August 22. IBM will make WebDialogs part of its Lotus division and add its service to the Sametime family of products, giving customers a software–as–a–service option for Web conferencing, the company said. Cisco and Microsoft are moving aggressively into unified communications, which combines all forms of interactive voice and data communications with presence technology that tells the world how a person can be reached in real time. IBM has taken a different approach, not building its own phone–switch replacement or a full range of communications tools, but ensuring compatibility with third–party products.

Source: <http://www.infoworld.com/article/07/08/22/IBM-buys-Web-confe>

36. *August 22, Reuters* — **Telecom offers reward for leads on copper theft.** U.S. rural telecommunications carrier Embarq is offering a \$5,000 reward for information leading to the arrest of anyone stealing its copper cables in Las Vegas amid a global crime spree targeting increasingly valuable metals. Embarq said on Wednesday, August 22, that copper cable theft has become a growing problem, particularly in Las Vegas, its largest market, where thieves have snipped away part of its aerial lines. The company, a spin-off from Sprint Nextel, has already spent \$400,000 so far this year to repair severed cable lines in Las Vegas. More than 60 people have been arrested in Las Vegas so far this year for stealing copper. Officials believe the stolen metal is sold as scrap to recycling centers. The price of copper has more than doubled over the past two years as rapid industrialization in China and other emerging economies spurred demand and triggered similar crimes around the world.

Source: [http://news.com/Telecom+offers+reward+for+leads+on+copper+theft/2100-1037\\_3-6203977.html](http://news.com/Telecom+offers+reward+for+leads+on+copper+theft/2100-1037_3-6203977.html)

37. *August 22, ComputerWorld* — **Storm Trojan horse may turn to hyping Hurricane Dean.** The 8-month old Storm Trojan horse may soon come full circle and take up touting Hurricane Dean, the Category 5 storm that slammed into Mexico Tuesday, August 21, security researchers said. Storm, also known as Peacomm, started life in January as malware attached to messages comprised of fake news accounts of a massive series of wind storms that struck Europe. One of the first Storm-bearing messages dangled the subject head "230 dead as storm batters Europe" to tempt users into launching the file. Recipients who clicked on the attached executable were infected by the Trojan horse, which turned their systems into spam-spewing zombies. Symantec Corp. researchers are betting that the malware's makers will try the same trick with Hurricane Dean.

Source: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032218&source=rss\\_topic85](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032218&source=rss_topic85)

### Internet Alert Dashboard

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

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

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

38. *August 23, New York Times* — **East St. Louis levees fail test.** The five levees that protect the metropolitan area of East St. Louis, IL, from the Mississippi River do not meet the Federal Emergency Management Agency's (FEMA) standards for flood protection and will be removed from maps that the agency publishes to record flood vulnerability, government officials said on Wednesday, August 22. The risk of the levees' failure is low, said Col. Lewis F. Setliff II, commander of the St. Louis District of the Army Corps of Engineers. But their inability to meet

the standards means that the flood maps will no longer show their presence. Instead, the area will be judged as if it is in an unprotected flood plain, officials said, and that in turn can have a powerful effect on housing costs, economic development and insurance rates. The assessment of those five levees is part of a nationwide effort to update flood maps, incorporating lessons learned from the flooding brought by Hurricane Katrina, said Terry Reuss Fell, regional chief of FEMA's floodplain management and insurance branch. The levees need repair and upgraded features like relief wells, which intercept the seepage, before they can meet the FEMA standards.

Source: [http://www.nytimes.com/2007/08/23/us/23levees.html?\\_r=1&oref=slogin](http://www.nytimes.com/2007/08/23/us/23levees.html?_r=1&oref=slogin)

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

## **General Sector**

Nothing to report.

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

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions: Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto: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](mailto: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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.