



Department of Homeland Security Daily Open Source Infrastructure Report for 24 July 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

- InformationWeek reports identifying information on more than half a million uniformed military personnel and their families was compromised by a military contractor that transmitted it over the Internet without encryption. (See item [8](#))
- ABC15 reports news investigators have discovered a 4.5–hour time frame each night when X–ray machines are off, metal detectors are closed, and virtually anything can be brought into the secure side of Phoenix Sky Harbor Airport. (See item [16](#))
- The U.S. Food and Drug Administration is expanding its July 18 warning for consumers and pet owners regarding canned food products and dog food produced by Castleberry Food Company of Augusta, Georgia, due to the risk of botulinum toxin. (See item [27](#))

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. *July 23, New York Times* — **Record failures at oil refineries raise gas prices.** Oil refineries across the country have been plagued by a record number of fires, power failures, leaks, spills, and breakdowns this year, causing dozens of them to shut down temporarily or trim production. The disruptions are helping to drive gasoline prices to highs not seen since last summer's

records. These mechanical breakdowns have created a bottleneck in domestic energy supplies, helping to push up gasoline prices 50 cents this year to well above \$3 a gallon. A third of the country's 150 refineries have reported disruptions to their operations since the beginning of the year, a record according to analysts. There have been blazes at refineries in Louisiana, Texas, Indiana, and California, some of them caused by lightning strikes. Plants have suffered power losses that disrupted operations; a midsize refinery in Kansas was flooded by torrential rains last month. After Hurricanes Katrina and Rita disrupted the nation's energy lifeline two years ago, oil companies delayed maintenance on many of their plants to make up for lost supplies and take advantage of the high prices. But, analysts say, they are now paying a price for deferring repairs.

Source: <http://www.nytimes.com/2007/07/22/business/22refine.html?ei=5065&en=652e82b4f396b467&ex=1185681600&adxnnl=1&partner=MYWAY&pagewanted=print&adxnnlx=1185164075-MdkH1nORYq2rJuOJy4TsMw>

2. *July 23, Associated Press* — **Peabody enlists help on proposed coal gasification plant.**

Peabody Energy has joined with a second company on a proposal to construct a \$3 billion coal-gasification plant that Kentucky lawmakers want to lure to their state with some \$300 million in tax breaks. Peabody said Monday, July 23, that ConocoPhillips would be a partner in the project to convert coal to synthetic natural gas. The proposal is to build the plant near an existing Peabody mine in Illinois, Indiana, or Kentucky. Feasibility studies are under way to determine the preferred location. The proposed plant would produce 50 billion to 70 billion cubic feet of pipeline quality synthetic natural gas per year from more than 3.5 million tons of coal. The project would include carbon capture and storage, "presuming there is a supportive regulatory framework in place." Peabody Energy is the world's largest private-sector coal company, with 2006 sales of 248 million tons of coal and \$5.3 billion in revenues. ConocoPhillips is an international, integrated energy company and one of the largest natural gas producers in North America.

Source: <http://www.kentucky.com/471/story/131059.html>

3. *July 23, Reuters* — **Japan accepts IAEA checks, nuclear policy on track.** Japan will work with United Nations inspectors to check the world's biggest nuclear power plant after a powerful earthquake last week caused radiation leaks, but a fundamental shift in its nuclear energy policy is unlikely despite renewed fears about nuclear safety. Japan had told the International Atomic Energy Agency (IAEA) that it did not need help for now, but on Monday, July 23, it said it would allow inspectors into the quake-hit Kashiwazaki-Kariwa plant after it came under pressure from local authorities to do so. Japan's nuclear industry — which supplies about one-third of the country's electricity needs and is central to its efforts to battle global warming — has been tarnished by cover-ups of accidents and fudged safety records. Chief Cabinet Secretary Yasuhisa Shiozaki said joint studies on nuclear safety would help other quake-prone countries as well as Japan.

Source: http://www.reuters.com/article/environmentNews/idUST21941820_070723

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

4.

July 22, Press–Enterprise (CA) — **Truck severs gas pipe, sparks towering fire.** A delivery driver ruptured a gas pipe in San Jacinto, CA, early Saturday, July 21, sparking a blaze that sent flames 30 feet in the air, burned for three hours and damaged a fast-food restaurant, authorities said. No injuries were reported, fire officials said. No evacuations were ordered, but police blocked off the southeast side of the strip mall near State Street and the Ramona Expressway for hours. The towering flames from the gas line stopped about 6:30 a.m. PDT when gas company workers finished digging two large holes in the parking lot, found the gas valves and shut them off.

Source: http://www.pe.com/localnews/sanjacinto/stories/PE_News_Local_S_hfire22.3c09428.html

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

Defense Industrial Base Sector

5. *July 23, Associated Press* — **Ammo industry prepares for slide.** The Lake City Army Ammunition Plant in Independence, MO, produces nearly 1.4 billion bullets a year, a dizzying figure driven by the demands of war. The question is, for how long? Although no one knows when the conflicts in Iraq and Afghanistan will end, ammunition industry executives understand the heavy orders won't last forever. So as they churn out the military's most essential pieces of hardware, ammunition makers are preparing for a downturn in business. They worry about a return to the post-Cold War period when the Pentagon slashed spending for small-caliber rifle rounds and other munitions, forcing suppliers to cut payrolls, mothball manufacturing equipment and lose hard-to-get environmental permits. Some closed their doors. "The demand is fast when it comes, and then it can drop off very quickly," said Karen Davies, Lake City's general manager. Military officials now talk about a need to protect the industrial base, but they also say it makes no sense to spend money for bullets and bombs the troops might not need.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/23/AR2007072300787.html>

6. *July 22, Aviation Week* — **Future bomber a foundation for next-gen gunship.** Air Force Special Operations Command (AFSOC) is planning to buy a fleet of bombers to house its future gunship, breaking with a decades-old tradition of using C-130 transports to carry heavy fires into the sky. Requirements for the Air Combat Command's bomber and the gunship are still being drawn up. But, both commands agree on some key characteristics: a degree of low observability — not necessarily full stealth — and endurance. The future gunship will look nothing like today's lumbering platform, and it could actually wind up appearing more like a B-2. "I don't think the transport next-generation gunship will be on a mobility platform because you are not going to need to carry around all that weight," says Lt. Gen. Michael Wooley, outgoing AFSOC commander. "If you are not carrying around that big gun and all of that heavy ammunition you don't need a big [transport] that is in itself vulnerable." ACC has announced it will not push the state-of-the-art for its next-generation bomber, which must be fielded beginning in 2018. That time frame and limited funding are prompting the Air Force to scale back earlier aspirations for a highly stealthy platform equipped with exotic directed-energy weapons.

Source: http://www.aviationweek.com/aw/generic/story_generic.jsp?cha

[nel=awst&id=news/aw072307p1.xml&headline=Future%20Bomber%20a%20Foundation%20for%20Next-Gen%20Gunship](http://news/aw072307p1.xml&headline=Future%20Bomber%20a%20Foundation%20for%20Next-Gen%20Gunship)

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

Banking and Finance Sector

7. *July 23, Associated Press* — **School conducts anti-phishing research.** The e-mail appeared to be a routine correspondence between two friends. "Check this out!" it read, then listed a Web address. But the note was fake. The catch? The scammers were Indiana University researchers, the e-mail an experiment. Methods at Indiana are raising ethical and logistical questions for researchers elsewhere: Does one have to steal to understand stealing? Can controlled phishing ever mimic real life? Indiana researchers say the best way to understand online security is to act like the bad guys. The university has conducted nearly a dozen experiments in the last two years. In one, called "Messin' With Texas," researchers learned mothers' maiden names for scores of people in Texas. Another conducted in May found that 72 percent of more than 600 students tested on the Bloomington, IN, campus fell for an e-mail from an account intended to look familiar that sought usernames and passwords. The experiments found that hackers have the most success by using hijacked Web addresses or e-mail accounts that look real. The research also showed computer users generally have little knowledge of Website security certificates and leave themselves open to attack with poorly configured routers or operating systems.

Source: http://news.yahoo.com/s/ap/20070723/ap_on_hi_te/phony_phishing;_ylt=As49zQqgJY.2FE5T7_yZxOkjtBAF

8. *July 23, InformationWeek* — **Information on 580,000 military personnel at risk.** Identifying information on more than half a million uniformed military personnel and their families was compromised by a military contractor. Science Applications International Corp. (SAIC), a Fortune 500 tech-services provider, released an advisory late last week that the company is notifying about 580,000 households, some with more than one affected person. The information, according to the release, was transmitted over the Internet without being encrypted. SAIC reported that it has forensic investigators trying to figure out if anyone actually grabbed any of the unencrypted information, adding that "the possibility cannot be ruled out." The information was stored on a single, SAIC-owned, non-secure server at a small SAIC location, and in some cases was transmitted over the Internet in an unencrypted form, according to the release. The contracts were with customers in the Departments of the Army, Navy, Air Force and Homeland Security.

Source: <http://www.informationweek.com/security/showArticle.jhtml;jsessionid=GMXILUFJIU3GAQSNDLRCKH0CJUNN2JVN?articleID=201200509>

9. *July 23, InformationWeek* — **Computer crimes charged in college cash-for-grades scheme.** Ten people, including the former director of admissions and the former director of the computer center at a Manhattan college, were indicted as being part of a scheme that involved forging transcripts and altering grades. Manhattan District Attorney Robert M. Morgenthau announced last week that the case centers around Touro College, where people who never attended classes at the school paid between \$3,000 and \$25,000 for forged transcripts. Three Touro College students also were indicted, along with three New York City Public School teachers. Andrique

Baron is charged with computer trespass, three counts of commercial bribe receiving in the first degree, seven counts of computer tampering in the third degree, and 10 counts of falsifying business records in the first degree. Michael Cherner is charged with computer trespass, two counts of commercial bribe receiving in the first degree, and one count of commercial bribe receiving in the second degree, one count of computer tampering in the third degree, and three counts of falsifying business records in the first degree.

Source: http://www.informationweek.com/security/showArticle.jhtml;jsessionid=GMXILUFJIU3GAQSNLDRCKH0CJUNN2JVN?articleID=20120042_9

10. July 23, *Government Accountability Office* — GAO-07-865: Information Technology: Treasury Needs to Strengthen Its Investment Board Operations and Oversight (Report).

The Department of the Treasury relies extensively on information technology (IT) to carry out its mission. For fiscal year 2007, Treasury requested about \$2.8 billion — the third largest planned IT expenditure among civilian agencies. GAO's objectives included (1) assessing Treasury's capabilities for managing its IT investments and (2) determining any plans the agency has for improving its capabilities. The Government Accountability Office (GAO) used its IT investment management framework (ITIM) and associated methodology to address these objectives, focusing on the framework's stages related to the investment management provisions of the Clinger-Cohen Act of 1996. To further strengthen Treasury's investment management capability, GAO recommends that the department develop and implement a plan to establish an executive investment review board and policies and procedures to manage nonmajor investments and address the other weaknesses GAO identified. In e-mail comments on a draft of this report, Treasury stated that the report reflects both Treasury's shortcomings as well as progress to date and recognized the need to take proactive steps to strengthen its investment board operations and oversight of information technology resources and programs.

Highlights: <http://www.gao.gov/highlights/d07865high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-865>

11. July 23, *IDG News Service* — Security hole in Fox News' Website reveals file directories and sensitive content. Security analysts spotted a gaping security hole in Fox News Network's Website on Monday, July 23, revealing file directories and sensitive content, although it appears the problem has been fixed. Several directories were visible on a server for Fox News that should normally not be accessible by a Web browser over the Internet. Also exposed was an FTP (File Transfer Protocol) connection to ziffdavis.com, plus a username and a password in a bash file, which is a Linux shell script used in this case to automatically login into an FTP server and grab news headlines. It would be hard to directly exploit the Web server, but being able to see how the Website is structured could open other ideas for an attack in the future.

Source: <http://www.infoworld.com/article/07/07/23/Fox-News-server-unsecured-1.html>

12. July 20, *eWeek* — Security firm discovers tool to make customized Trojans. A security firm has uncovered an easy-to-use, affordable tool for making a variety of customized Trojans — from downloaders to password stealers — on sale at several online forums. The tool, discovered by PandaLabs, is called Pinch, a tool that allows cybercriminals to specify what type of password they want their Trojans to steal. Pinch also has encryption capabilities to ensure that nobody intercepts stolen data. Pinch's interface also has a SPY tab that lets criminals turn Trojans into keyloggers. In addition, the tool can design Trojans that snap screenshots from infected computers, steal browser data and look for specific files on the target system. Pinch is

impressive, but it's just one sample of the array of crimeware for sale in malware markets and covered in a recent report from PandaLabs titled "The Price of Malware." Malware has, in fact, increased 172 percent over the past years, according to the security firm. PandaLabs has tracked several instances of the use of malware in the past few months: One example is a variant of the Briz Trojan, called Briz.X, that had already stolen over 14,000 users' bank account information by the time it was detected.

Source: <http://www.eweek.com/article2/0.1895.2161000.00.asp>

13. *June 22, Government Accountability Office* — **GAO-07-705: Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats (Report)**. Computer interconnectivity has produced enormous benefits but has also enabled criminal activity that exploits this interconnectivity for financial gain and other malicious purposes, such as Internet fraud, child exploitation, identity theft, and terrorism. Efforts to address cybercrime include activities associated with protecting networks and information, detecting criminal activity, investigating crime, and prosecuting criminals. The Government Accountability Office's (GAO) objectives were to (1) determine the impact of cybercrime on our nation's economy and security; (2) describe key federal entities, as well as nonfederal and private sector entities, responsible for addressing cybercrime; and (3) determine challenges being faced in addressing cybercrime. To accomplish these objectives, GAO analyzed multiple reports, studies, and surveys and held interviews with public and private officials. GAO recommends that the Attorney General and the Secretary of Homeland Security help ensure adequate law enforcement analytical and technical capabilities. In written comments on a draft of this report, the FBI and the U.S. Secret Service noted efforts to assess and enhance these capabilities. Highlights: <http://www.gao.gov/highlights/d07705high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-705>

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

Transportation and Border Security Sector

14. *July 23, Chicago Sun-Times* — **Two arrested after forced O'Hare landing**. A flight bound for San Francisco from Boston was forced to land at O'Hare Airport on Sunday, July 22, after two passengers allegedly harassed another person aboard the plane. Joseph A. Koschitzki, 60, and Terri Binder Koschitzki, 53, were arrested on charges of simple battery, according to Chicago Police News Affairs Sgt. Eugene Mullins. The two are from Thousand Oaks, CA. Department of Aviation spokesperson Gregg Cunningham said the incident occurred aboard United Airlines Flight 173. The plane was diverted to O'Hare and landed about 10:20 a.m. CDT. "The couple refused to comply with flight crew orders," Cunningham said.
Source: <http://www.suntimes.com/news/metro/479909.CST-NWS-hare23.article>
15. *July 23, Associated Press* — **Washington, DC airports consider security fast lanes**. The Metropolitan Washington Airports Authority issued a request last month for companies that would install, manage and operate a Registered Traveler Program at its airports. The agency oversees Reagan National and Dulles International airports. The security measure was tested in pilot programs in 2005. It is being gradually implemented in some cities by the Transportation Security Administration. Under the program, passengers who pass an extensive background check would receive a card to go through a faster security line. The line would include

precautions such as a retinal or fingerprint scan.

Source: http://www.wusa9.com/news/news_article.aspx?storyid=61062

16. July 23, ABC15 (AZ) — Security questions at Phoenix Sky Harbor Airport. News investigators have discovered a 4.5-hour time frame each night when virtually anything can be brought into the secure side of Phoenix Sky Harbor Airport. The X-ray machines were off, the metal detectors were closed, and bags with unknown contents were carried to the secure side of the airport where the planes are. ABC15 Investigators watched as a security guard let people with purses, coolers and suitcases walk right through — bags unchecked. Documents obtained by the ABC15 Investigators show officials have known for two years that this is going on. In 2005, airport officials hired an outside company to handle security during the times when passenger flights are done for the day. The documents said the guards would not search personal items or the people. One on-duty security guard said it was hard sometimes to keep from falling asleep. When the clock strikes 4:30 a.m. the Transportation Security Administration takes over. The X-ray machines are back on, the metal detectors are working, and everyone, including incoming employees just like the ones we watched all night long, are screened. Airport security expert Larry Wansley said this situation needs to be fixed immediately.

Source: http://www.abc15.com/news/local/story.aspx?content_id=568d6b4d-67b7-4116-9098-4c35d8b5ce38#top

17. July 23, Department of Transportation — Department of Transportation provides loan for Virginia airport connector. An airport connector near Richmond — a planned segment of the Pocahontas Parkway that was never built due to insufficient funds — will be built, thanks to a \$150 million loan from the Department of Transportation's Federal Highway Administration. “The reality of current funding and the growing demand on America's transportation network calls for new ways of financing our transportation infrastructure,” said Transportation Secretary Mary E. Peters. The loan would be applied toward the \$798 million cost of the entire project, which includes the cost of building the Richmond Airport Connector. The loan is made possible by the Transportation Infrastructure Finance and Innovation Act of 1998.

Source: <http://www.dot.gov/affairs/fhwa0907.htm>

18. July 22, Central Florida News 13 — Bomb threat causes delays at OIA. A threatening note was found on board a flight bound for Boston at Orlando International Airport (OIA) Sunday afternoon, July 22. AirTran Flight 515 was getting ready to take off when the note was found on board tucked inside a magazine. Everyone was then taken off the plane. The FBI searched the jet, in addition to all the luggage and passengers, but nothing suspicious was found. The plane was able to take off about three hours later.

Source: http://www.cfnews13.com/News/Local/2007/7/22/airtran_bomb_sc_are.html

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

Postal and Shipping Sector

19. July 21, Associated Press — Five people taken to hospital following suspicious envelope powder. A suburban Chicago JP Morgan Chase bank building was quarantined on Saturday,

July 21, and five people were taken to a hospital after a suspicious powder was found inside an envelope. Elgin spokesperson Sue Olafson said tests later showed that the powder was sugar. Olafson says the envelope had apparently been mistakenly delivered to the building and leaked a gray powder. Several people complained about feeling ill, including five people who were transported to a hospital. Olafson said the letter appeared to come from India.

Source: <http://www.wqad.com/Global/story.asp?S=6822054&nav=1sW7>

[[Return to top](#)]

Agriculture Sector

20. *July 23, USAgNet* — Apple moths spread in California. The light brown apple moth, which was spotted in San Francisco earlier this year, has spread to other areas in California, state officials say. The moth, a pest that attacks a variety of crops, was previously detected in nine San Francisco and Central Coast counties, according to the California Department of Food and Agriculture. But other areas including Sherman Oaks and Solano County in northern California also reported sightings of apple moths, it said.

Source: <http://www.usagnet.com/story-national.php?Id=1686&yr=2007>

21. *July 23, Stop Soybean Rust News* — Asian soybean rust found in Mexico. Mexican officials have confirmed the presence of Asian soybean rust on yam bean leaves in the state of Veracruz in January, 2007. According to a report posted July 12, 2007, on the North American Plant Protection Organization's Phytosanitary Alert System, "by the middle of January 2007, the Plant Health General Directorate received samples of yam bean (*Pachyrhizus erosus*) crop foliage from the communities of Agua Dulce and Pajapan, in Papantla township, in the state of Veracruz. These samples showed signs and symptoms of Asian soybean rust (*Phakopsora pachyrhizi*)." Veracruz is in east-central Mexico, on the Gulf of Mexico. It is one state south of the state of Tamaulipas and one state east of San Luis Potosi, both of which had Asian soybean rust on soybean leaves in February, 2006.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=1068>

22. *July 20, Animal and Plant Health Inspection Service* — USDA proposes to adjust user fees for veterinary diagnostic services. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service Friday, July 20, announced a proposal to adjust the user fees charged for veterinary diagnostic services. These user fees would be increased incrementally during fiscal years 2008 to 2012 to reflect the anticipated costs associated with providing diagnostic services each year. APHIS currently charges fees for its veterinary diagnostic services, or the laboratory work involved in identifying and diagnosing disease-causing organisms or chemical agents in animals. Specifically, APHIS is proposing to adjust the fees for the following services: Laboratory tests, reagents and other veterinary diagnostic services performed at the National Veterinary Services Laboratories' (NVSL) Foreign Animal Disease Diagnostic Laboratory; Laboratory tests performed as part of isolation and identification testing at NVSL; Laboratory tests performed as part of serology testing at NVSL; Laboratory tests performed at the pathobiology laboratory at NVSL; Diagnostic reagents produced at NVSL or other authorized sites; and Other diagnostic services or materials provided at NVSL.

Source: <http://www.aphis.usda.gov/newsroom/content/2007/07/vetdfees.shtml>

23. *July 19, Business First (NY)* — **Fruit trees under quarantine in Niagara.** Two areas of western Niagara County, NY, have been placed under agricultural quarantine because of a disease that attacks certain commercial and ornamental fruit trees. The plum pox virus has caused a moratorium to be imposed on portions of the towns of Porter and Wilson that bans planting several species of stone fruit trees, including peach, plum, nectarine, apricot and cherry, which are susceptible to the disease. It is also unlawful to plant certain ornamental trees and shrubs. The disease is believed to have originated in Europe and was imported during the 1980s and 1990s into Pennsylvania and Ontario in Canada. To determine if the disease has spread beyond the quarantined areas, a three-year survey was launched by the U.S. Department of Agriculture and the state Department of Agriculture and Markets. The survey, which will include questionnaires and collecting leaf samples, will contact residents as well as orchard and nursery operators in areas up to five miles around the quarantined areas.

Source: <http://washington.bizjournals.com/buffalo/stories/2007/07/16/daily40.html>

24. *July 19, Prince Albert Daily Herald (Canada)* — **Anthrax found near Prince Albert.** The Canadian Food Inspection Agency (CFIA) is reporting a case of anthrax in a cow that died Friday, July 13, in Torch River. Sandra Stephens, an agency spokesperson, said results from a test conducted by a Prince Albert-area veterinarian were sent to a laboratory in Saskatoon, where the case was confirmed. After the CFIA was notified, the agency ensured the infected cow's remains were disposed of and the rest of the 100-some cattle in the herd were placed under a three-week quarantine.

Source: <http://www.paherald.sk.ca/index.cfm?sid=46081&sc=4>

[[Return to top](#)]

Food Sector

25. *July 21, Food Safety and Inspection Service* — **Michigan firm recalls ground beef products.** Abbott's Meat Inc., a Flint, MI, establishment, is voluntarily recalling approximately 26,669 pounds of ground beef products because they may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Saturday, July 21. The problem was discovered through routine FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of these products. The ground beef products were produced between July 12 and July 20, 2007 and were distributed to hotels, restaurants and institutions in Michigan. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration. The very young, seniors and persons with compromised immune systems are the most susceptible to foodborne illness.

Source: http://www.fsis.usda.gov/News_&_Events/Recall_034_2007_Releas/index.asp

26. *July 21, Los Angeles Times* — **Warning issued on a type of candy from Mexico.** The California Department of Public Health warned consumers Friday, July 20, not to eat a certain type of candy imported from Mexico because it contains "high levels of lead." The warning pertains to De La Rosa Pulparindo candy.

Source: <http://www.latimes.com/news/printedition/california/la-me-sb-riefs21jul21.1.6768970.story?coll=la-headlines-pe-california>

27. *July 21, U.S. Food and Drug Administration* — **FDA Expands Its Warning about the Risk of Botulism poisoning from certain Castleberry food products and dog food.** The U.S. Food and Drug Administration (FDA) is expanding its July 18 warning to consumers. This expansion is for consumers and pet owners regarding canned food products and dog food produced by Castleberry Food Company of Augusta, GA, due to the risk of botulinum toxin. The agency is expanding its warning based in part on FDA test results and information obtained during a joint FDA and U.S. Department of Agriculture inspection of the Castleberry's facility in Augusta, GA. Exposure to botulinum toxin can be fatal and two people in Texas and two people in Indiana remain seriously ill and hospitalized with botulism poisoning associated with eating Castleberry's Hot Dog Chili Sauce. While the previous recall and the known illnesses are linked to production dates of April 30 to May 22, 2007, the firm has extended the recall to include all products irrespective of "best by" date. In addition, Castleberry is recalling other products containing meat, which are regulated by the U.S. Department of Agriculture.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01670.html>

28. *July 21, Associated Press* — **Woman charged with tainting soup.** A woman has been accused of dropping mothballs into a vat of soup at an Austin, TX, grocery store deli after investigators traced her through a store savings card. Lea Suzan Sechler, faces a felony charge of tampering with a consumer product. She was released on bail after her arrest Thursday, July, 19. She had been a regular customer at the Randall's supermarket where at least three times customers and employees noticed the soup had the scent of mothballs. Authorities say a deli clerk noticed a mothball smell coming from the soup in late May and was told to throw it out. About a week later, a customer complained about a smell coming from soup she bought at the store. A manager closed the soup station and sent the batch for testing at a food industry safety company, an affidavit said. The soup tested positive for dichlorobenzene, a primary ingredient in many mothballs. Management at the supermarket installed surveillance cameras near the soup station after the second incident. A manager noticed the smell of mothballs again on June 20. Surveillance video showed Sechler opening a vat of soup at the cart before it started to smell, police said.

Source: <http://www.chron.com/disp/story.mpl/ap/tx/4987671.html>

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

Water Sector

29. *July 23, Associated Press* — **Construction starts on Santa Cruz pilot desalination plant.**

Construction has begun on a pilot desalination plant that could turn ocean water into drinking water by the end of the year. The city and Soquel Creek Water District are building the \$4 million pilot desalination plant at the University of California, Santa Cruz, Long Marine Laboratory. The 2,400-square-foot test facility is expected to pump 72,000 gallons of sea water a day. If it passes environmental scrutiny, city water officials and the water district may build a \$40 million permanent desalination facility.

Source: http://www.mercurynews.com/news/ci_6442355

30. *July 22, Denver Channel* — **Mandatory water restrictions placed on 59,000 Colorado homes.** A mandatory water restriction was placed on about 59,000 households in Longmont and east of Carter Lake and other surrounding areas following a chemical explosion at the

Carter Lake Water Treatment Plant on Friday, July 20. The restriction says residents are to refrain from watering of any kind outside their homes and are to limit any indoor watering to necessary use only, said Capt. Scott Lindschmidt of the Berthoud Fire Department. Officials said two combustible chemicals were accidentally mixed and are what caused part of the treatment facility to explode.

Source: <http://www.thedenverchannel.com/news/13732319/detail.html>

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

Public Health Sector

31. July 23, Associated Press — Teen with meningitis on AirTran flights. A teenager who fell seriously ill on an AirTran Airways flight was diagnosed with bacterial meningitis, and the airline was contacting passengers who sat near her, a spokesperson said. The girl was in critical condition Monday, July 23, a hospital spokesperson said. The teen had traveled Saturday, July 21, from Orlando, FL, to Atlanta, GA, on Flight 862 and then to Wichita, KS, on Flight 687, AirTran spokesperson Dave Hirschman said. Meningitis, a bacterial infection of the lining surrounding the brain and spinal cord, primarily affects children, killing about 10 percent of those infected.

Source: http://seattlepi.nwsourc.com/national/1110AP_AirTran_Meningitis.html

32. July 22, Agence France–Presse — Asia braces for new dengue outbreak. From rich Singapore to impoverished Cambodia, public health officials are warning of a possible epidemic of dengue fever in Asia this year. The World Health Organization (WHO) believes 2007 could be on a par with 1998, when nearly 1,500 people died in Asia of the mosquito-borne disease. This year dengue has already killed more than 1,000 people in Indonesia alone. In many other places the death and infection rates through June had already surpassed the totals for 2006. In Cambodia, deaths this year have already eclipsed fatalities in 2006 as the country battles one of the worst outbreaks of the disease in a decade. Some 182 deaths have been recorded for the six months of the year out of nearly 15,000 cases, said Ngan Chantha, director of the health ministry's dengue program. Last year 152 deaths were reported. Vietnam has reported almost 20,000 cases with 21 deaths, seven more than in the same period last year, the health ministry said.

Source: http://news.yahoo.com/s/afp/20070723/hl_afp/healthasiadengue_070723062522;_ylt=AvMaNbKYqSLCib191.Sn14CJOrgF

33. July 22, Reuters — Egyptian woman tests positive for bird flu. A 25-year-old Egyptian woman has tested positive for the deadly H5N1 bird flu virus, bringing the number of human cases in the most populous Arab country to 38, a World Health Organization official said on Sunday, July 22. Egypt's state news agency MENA reported she was from the Nile Delta province of Damietta, in northern Egypt. It said she developed a high fever on Friday, July 19, and was in good condition after receiving the antiviral drug Tamiflu. Since bird flu first emerged in Egyptian poultry last year, 15 Egyptians have died from the virus.

Source: <http://africa.reuters.com/wire/news/usnL22411713.html>

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

Government Sector

34. *July 22, Government Accountability Office* — **GAO-07-658: Federal Real Property: DHS Has Made Progress, but Additional Actions Are Needed to Address Real Property Management and Security Challenges (Report)**. The Department of Homeland Security (DHS) has 10 major organizational components that include more than 27,000 owned or leased buildings and structures totaling about 78 million square feet. About 72 percent of DHS real property is federally owned, while about 28 percent of DHS real property is federally leased. The U.S. Coast Guard has the majority of DHS real property, accounting for 69 percent of its buildings and about 41 percent of its square footage. The Government Accountability Office's (GAO) objectives were to (1) describe DHS's real property portfolio; (2) determine what challenges, if any, DHS faces in managing real property and what actions it has taken in response to the administration's real property initiative; (3) determine what challenges DHS and the General Services Administration (GSA) face in consolidating DHS's Washington, DC headquarters; and (4) describe actions DHS has taken to help ensure the security of its facilities. In recent years, DHS has taken actions intended to improve the security of its facilities, but its efforts fall short in certain key areas. DHS has designated a Chief Security Officer for the department and has established a Chief Security Officer Council to evaluate security issues. Highlights: <http://www.gao.gov/highlights/d07658high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-658>

[[Return to top](#)]

Emergency Services Sector

35. *July 23, Sun Herald (MS)* — **Mock exercise to help prepare first responders in Biloxi**. City officials in Biloxi, MS, will meet Tuesday morning, July 24, for a tabletop exercise to make sure all the "what ifs" in their emergency responsive plan are in check when another hurricane hits. Led by Jay Williams, the city's new emergency management director and veteran firefighter, department heads and city managers will set up an incident command system at City Hall for the mock exercise. Department heads have been meeting almost weekly in anticipation of the discussion, which will include making sure important files are stored, police cruisers and city vehicles are gassed, cell phones are charged, with backup battery packs stowed, City Manager Richard Rose said. Department leaders will need to use City Hall as the central command center for another emergency. Officials will also prepare for any unexpected incidents that might arise before the storm, such as a gas leak or a house fire, that could interfere with the emergency response plan. All department heads from police and fire, public works, parks and recreation, city hall and zoning and planning will attend.
Source: <http://www.sunherald.com/201/story/104023.html>
36. *July 22, Asbury Park Press (NJ)* — **Experts say New Jersey coast due for a hurricane**. From what he's been told, "we are due" for a hurricane in New Jersey, said Richard L. Canas, director of the state Office of Homeland Security and Preparedness. "They seem to come around in cycles, and we haven't had one here in quite a while." State officials say hurricane planning has improved since last year. Meanwhile, the public's response to evacuation orders is a key issue, officials say. "The biggest problem for us is getting people to actually move when we tell them

to move, and that seems to be a problem not only for us but for other areas also," said Oceanport police Captain Mauro Baldanza, borough emergency management coordinator. It will take about eight to 10 hours to evacuate people from areas prone to storm surges in Ocean, Atlantic and Cape May counties, which have barrier islands, and six hours in Monmouth County, said Della Fave, of the State Police. It would take a maximum of 44 hours for "the very last vehicle" to reach Pennsylvania or New York from Ocean, Atlantic or Cape May counties, Della Fave said. The figure is slightly less in Monmouth County.

Source: <http://www.app.com/apps/pbcs.dll/article?AID=/20070722/NEWS/707220386/1001/DWEK01>

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

Information Technology and Telecommunications Sector

37. July 23, IDG News Service — HP to acquire Opware for \$1.6 billion. Hewlett-Packard (HP) plans to buy datacenter automation software vendor Opware for about \$1.6 billion. It's the third-largest acquisition in HP's history after its multibillion-dollar purchases of Compaq and Mercury. HP said Monday, July 23, that it had signed a definitive agreement to acquire Opware in a cash tender deal that values the company at \$14.25 per share. Once the deal closes, HP plans to combine the Opware software with its own enterprise IT management software, as the new acquisition becomes part of HP's software business.

Source: http://www.infoworld.com/article/07/07/23/HP-to-acquire-Opware_1.html

38. July 23, IDG News Service — Security team claims successful iPhone hack. A team of security experts in Baltimore said it has found a flaw in Apple's iPhone handset that can be used by attackers to access private data stored on it. Independent Security Evaluators (ISE) said on a Website dedicated to explaining the flaw and its exploitation that an attacker could gain access to the iPhone through a wireless access point, or through a Website controlled by the attacker. Because the iPhone connects to wireless Internet access networks, such as Wi-Fi, by name, an attacker could create a network with the same name and encryption method as one the handset already uses. The attacker could then substitute a Web page with exploit code to gain access to the phone, ISE said. An attacker could also use a link planted on an unedited or unmoderated online forum, or a link sent by SMS or e-mail to use make use of the flaw and gain access to the handset, ISE said. When the iPhone's Safari browser opens a malicious Web page, malicious code can be run on the phone via the flaw, allowing the attacker to read the iPhone's SMS log, address book, call history, and voice-mail information, ISE said.

Source: http://www.infoworld.com/article/07/07/23/successful-iPhone-hack_1.html

39. July 23, VNUNet — Symantec warns of cross-platform vulnerability. Symantec has warned of an exploit in circulation that can crash Nintendo's Wii gaming console. The problem concerns the use of Flash files on the console. Adobe patched the Flash flaw on July 12, but the Opera browser used by the Wii is still vulnerable. "The most interesting thing is that it is a cross-platform vulnerability," said Liam OMurchu from Symantec's Security Response team. "Due to the fact that Flash can run in different browsers and on different platforms, the discovery of this one vulnerability could leave all Flash-enabled operating systems and devices open to the attack, including some advanced smartphones. The vulnerability has already been tested on Windows, Apple Mac, and some Linux distributions, but many other devices that are

Flash-enabled could be affected by the problem too."

Source: <http://www.vnunet.com/vnunet/news/2194782/symantec-warns-wii-flaw>

40. *July 20, eWeek* — **Duke resolves iPhone, Wi-Fi outage problems.** One week after discovering a glitch between Apple iPhones and its Cisco-based campus wireless network, Duke University on Friday, July 20, finally got to the bottom of the problem that caused periodic outages of the Wi-Fi network. Initial reports of the problem placed the blame for the outages squarely on Apple's iPhones, which flooded the Cisco Wireless Access Points with thousands of address requests per second. However, in a statement released Friday afternoon, Cisco Systems admitted that the problem was caused by a Cisco glitch. "Cisco has provided a fix that has been applied to Duke's network and the problem has not occurred since," the statement read. Cisco did not describe what the source of the problem was.
- Source: <http://www.eweek.com/article2/0.1895.2161065.00.asp>

Internet Alert Dashboard

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

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

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[[Return to top](#)]

General Sector

41. *July 18, Zanesville Times Recorder (OH)* — **Metal theft is becoming an international problem.** According to Zanesville (Ohio) Police Detective Ric Roush and Josh Joseph, Muskingum Iron and Metal Co. vice president and owner, the theft of copper, aluminum, and metal objects is becoming an international problem. When Roush said his department got more than a dozen reports of catalytic converters being stolen off trucks and vans parked overnight in various lots around the city, he started looking into the problem and discovered it is not only city wide or even state wide, but has become an international problem. Joseph, who is also a past president of the Institute of Scrap Recycling Industry, agreed with Roush and said the problem is "growing world wide." This is due to very high metal prices, Joseph said. Thieves are taking everything from manhole covers to urns from cemeteries to sawing copper wiring out of homes under construction. Currently Joseph and Ohio Senator Steve Stivers are working on House Bill 171 that will limit what scrap dealers can take.
- Source: <http://zanesvilletimesrecorder.com/apps/pbcs.dll/article?AID=/20070718/NEWS01/707180304/1002>

[[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.