



# Department of Homeland Security Daily Open Source Infrastructure Report for 23 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

- Information Week reports a former U.S. Marine and FBI analyst was sentenced to 10 years in federal prison for espionage charges in connection with stealing classified national defense documents from the White House, the FBI, the Department of Defense, and the U.S. Department of State. (See item [27](#))
- The Associated Press reports the blast that made New York skyscrapers tremble on Wednesday, July 17, came from an 83-year-old steam pipe and sent a powerful message that the miles of tubes, wires, and iron beneath New York and other U.S. cities are getting older and could become dangerously unstable. (See item [37](#))

### 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 22, Arizona Star* — **Mexico's vulnerable pipelines could face new hits.** When saboteurs blew up several natural gas pipelines in central Mexico this month, temporarily shutting down production for U.S. automakers and other important manufacturers, a small and shadowy Marxist guerrilla group called the Popular Revolutionary Army reportedly claimed responsibility. Mexico's guerrilla movements historically have been small in scale and generally amount to a political nuisance, so attacks on pipelines are highly unusual. But, if it isn't the

EPR, the question then is who is behind the bombings? Mexico is the second-largest exporter of crude oil to the United States — more than 1.4 million barrels per day as of April — and if unknown assailants can blow up a natural gas pipeline, they could strike as easily at oil. World oil prices are now above \$73 a barrel, and further strikes against Mexican energy infrastructure would add to the price jitters. Mexico is a dangerously soft target since it has more than 17,000 miles of oil pipelines and 8,235 miles of natural gas pipelines to protect. A McClatchy Newspapers investigation in March demonstrated that Mexico's oil installations can be accessed without authorization.

Source: <http://www.azstarnet.com/news/192824>

- 2. July 20, Associated Press — FPL to convert citrus waste into ethanol.** An FPL Group subsidiary says it will develop a first-of-its-kind commercial plant to convert orange and grapefruit waste into ethanol that will be sold to Florida motorists at gasoline pumps "Currently, there is no ethanol production in Florida," said David Stewart, president of Boca Raton-based Citrus Energy LLC, a partner in the development of the FPL Energy ethanol plant. "This is the first in the world for citrus." State Agriculture Commissioner Charles Bronson said the proposed facility is one of several now being discussed to move Florida from the sidelines of ethanol production to the forefront of developing more efficient ways of making the alternative fuel. The FPL plant is expected to produce about four million gallons of ethanol a year to be sold as a gasoline additive in Florida. The plan is to build it in Hendry County, an agricultural region just south of Lake Okeechobee. FPL Energy is a subsidiary of FPL Group Inc., which also operates the state's largest utility, Florida Power & Light Co.

Source: [http://biz.yahoo.com/ap/070720/fl\\_citrus\\_ethanol\\_plant.html?.v=1](http://biz.yahoo.com/ap/070720/fl_citrus_ethanol_plant.html?.v=1)

- 3. July 20, Platts Energy Bulletin — Constellation and EDF partner to build new nuclear in U.S.** Baltimore-based Constellation Energy and Electricite de France (EDF) have agreed to a 50-50 joint venture to develop, deploy, own, and operate nuclear power plants in the U.S., the companies announced July 20. In an interview, Michael Wallace — Constellation's executive vice president and the president of the company's Generation Group — said \$175 million was tied to the filing of applications with the Nuclear Regulatory Commission for combined construction permit-operating licenses.

Source: <http://www.platts.com/Nuclear/News/7533750.xml?sub=Nuclear&p=Nuclear/News&?undefined&undefined>

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

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

- 4. July 20, WFAA (TX) — Carbon monoxide leak forces evacuations.** A report of carbon monoxide fumes led to the evacuation of a strip shopping center, dialysis center and play group in Oak Cliff, TX, Friday morning, July 20. Dallas Fire-Rescue investigators confirmed the presence of the odorless and potentially deadly gas. There were no reports of injuries. The leak came from a hot water heater in the dialysis center.

Source: [http://www.wfaa.com/sharedcontent/dws/news/localnews/tv/stories/wfaa070720\\_wz\\_coevac.92c096ff.html](http://www.wfaa.com/sharedcontent/dws/news/localnews/tv/stories/wfaa070720_wz_coevac.92c096ff.html)

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

## Defense Industrial Base Sector

Nothing to report.

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

## Banking and Finance Sector

5. *July 20, Websense Security Labs* — **Phishing Alert: Tiscali UK.** Websense Security Labs has received reports of a phishing attack that targets customers of Tiscali UK. Users receive a spoofed e-mail message claiming that their most recent bill payment could not be processed. The e-mail provides a link to a phishing site, which attempts to collect personal and account information. This phishing site is hosted in the United Kingdom and was up at the time of this alert.  
Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=789>
  
6. *July 20, InformationWeek* — **Federal prosecutor: Cybercrime is funding organized crime.** For months now, the government has said organized crime was moving into the realm of cybercrime, using hackers to run scams and break into systems. But Assistant U.S. Attorney Erez Liebermann, chief of the computer hacking and intellectual property section in New Jersey's U.S. Attorney's Office, says cybercrime has been so profitable for organized crime that they're now using it to fund the rest of their underground operations. "In terms of the risks and rewards, there's a higher chance of getting more, financially, using the world of computer crime. Organized crime is realizing this," he said. "We have suspicions of organized crime being behind some cybercrime that we're investigating here." Analysts at Websense, a Web security company, reported late last year that the mob was expected to band together more closely with hackers in 2007 to form a more organized cybercrime community. The beefed-up online crime cooperative has begun buying, selling, and trading ready-made cyberattack toolkits and exploiting zero-day vulnerabilities. Dan Hubbard, VP of security research at Websense, noted that organized criminals have realized that the Internet has been an untapped resource for earning them profit.  
Source: <http://www.informationweek.com/security/showArticle.jhtml;jsessionid=2KPJMUB1VAATKQSNLPSKHSCJUNN2JVN?articleID=201200167&articleID=201200167>
  
7. *July 19, Associated Press* — **Grand jury indicts 17 people for stealing personal information.** A federal grand jury has indicted 17 people for allegedly using the identities of Kansas City, MO-area nursing home residents to file bogus tax returns across the country. They allegedly sought \$13.1 million in refunds. In an indictment returned Wednesday and unsealed Thursday, July 19, prosecutors charge the defendants with stealing the personal information of around 300 individuals and using it to file at least 365 fraudulent federal tax returns beginning as far back as February 2005. U.S. Attorney John Wood told reporters the conspirators also filed fraudulent tax returns in 27 states. Wood said some of the refunds paid to the defendants were cashed and transferred to the African nation of Kenya, where 12 were either born or held citizenship.  
Source: <http://www.kctv5.com/news/13717800/detail.html>

8. *July 19, Register (UK)* — **Governments' systems used to power phishing push.** Lax security controls are allowing con men to host fraudulent Websites on servers run by government organizations and private sector firms. For example, Symantec has detected a number of phishing sites that have been hosted on government URLs over recent months. In June alone, fraudulent sites were identified on sites run by the governments of Thailand, Indonesia, Hungary, Bangladesh, Argentina, Sri Lanka, the Ukraine, China, Brazil, Bosnia and Herzegovina, Colombia, and Malaysia. The quantity of phishing sites hosted on government systems flies in the face of the perceived wisdom that government systems are more secure. "Hosting a phishing Web page on a government site has a number of advantages for a phisher. Government Websites often receive a high volume of traffic, so their servers can handle the extra traffic generated by a phishing site," writes Symantec researcher Nick Sullivan. "This extra traffic might not be noticed immediately, giving the phishing site a longer lifespan before it is detected and shut down. Perhaps most importantly, hosting a phishing site on an actual government URL gives the phishing site a sense of authenticity that's hard to beat." Symantec blog: [http://www.symantec.com/enterprise/security\\_response/weblog/2007/07/government\\_servers\\_hosting\\_phi.html](http://www.symantec.com/enterprise/security_response/weblog/2007/07/government_servers_hosting_phi.html)  
Source: [http://www.theregister.co.uk/2007/07/19/govt\\_phishing\\_hosts/](http://www.theregister.co.uk/2007/07/19/govt_phishing_hosts/)

9. *July 19, Reuters* — **U.S. arrests ex-Samsung employee for embezzlement.** A former director at a Samsung Corp. unit was arrested on a wire fraud charge Thursday, July 19, on allegations that he had embezzled about \$1.5 million from the company, U.S. prosecutors said. John Y. Lee, 44, who was a director at Samsung America Inc.'s Korea Export Department, was fired by the company after the alleged scheme came to light, the U.S. Attorney's office in New Jersey said in a statement. Lee allegedly engaged in an elaborate scheme between 2002 and 2007 to embezzle the money, prosecutors said. He created a fictitious entity and falsified various documents including purchase orders, invoices and approval forms to make it appear as though the entity were providing metal refining services to Samsung Corning Precision Glass Co. Ltd., a joint venture of Samsung Corp. and Corning Inc., prosecutors alleged. Lee, who received about \$1 million from Samsung America through the scheme, spent the money on personal expenses, including for a down payment on a house in Fort Lee, New Jersey, prosecutors said. Source: <http://www.eweek.com/article2/0.1895.2160546.00.asp>

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

## **Transportation and Border Security Sector**

10. *July 22, Associated Press* — **Texas flooding strands passenger train.** Storms dumped more than a foot of rain on parts of Texas, stranding more than 170 passengers on an Amtrak train for hours and forcing rescue crews elsewhere to pull at least 50 people to safety. Water covering the tracks in Knippa, TX, about 75 miles west of San Antonio, stopped a westbound Amtrak train carrying 176 passengers at around 9 a.m. CDT on Saturday, July 21, authorities said. Amtrak spokesperson Vernae Graham said buses were driving the passengers to El Paso, where they would board another train early Sunday. The train never lost power, but buses could not reach it until early Saturday evening because of flooded roads, Graham said. No serious injuries were reported in the state's latest round of flooding, which closed many roads and forced evacuations.

Source: <http://hosted.ap.org/dynamic/stories/F/FLOODING?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT>

**11. July 21, Associated Press — Brazil's aviation radar goes dark.** A radar failure over the Amazon forced Brazil to turn back or ground a string of international flights Saturday, July 21, deepening a national aviation crisis just hours after the president unveiled safety measures prompted by the country's deadliest air disaster. Further shaking Brazilians' confidence, authorities announced that they had mistaken a piece of the fuselage from that accident for the flight recorder and sent it to a laboratory for analysis. The radar outage from 11:15 p.m. Friday to 2:30 a.m. Saturday (local time), caused by an electrical problem, forced numerous planes heading to Brazil from the United States to return to their points of origin and make unscheduled landings at airports from Puerto Rico to Chile. Eight of the 17 planes flying in the coverage area of the radar system were rerouted, and some airlines canceled flights bound for Brazil. While the nation has had chronic problems with delays and cancellations on domestic flights over the past 10 months, the radar outage was the first time that international flights have been severely affected.

Source: <http://www.cnn.com/2007/WORLD/americas/07/21/brazil.aviation.ap/index.html>

**12. July 20, Government Accountability Office — GAO-07-718: Intermodal Transportation: DOT Could Take Further Actions to Address Intermodal Barriers (Report).** Intermodal transportation enables freight and passengers to cross between different modes of transportation efficiently and can improve mobility, reduce congestion, and cut costs. In 1991 Congress called for a National Intermodal Transportation System and created the Office of Intermodalism within the Department of Transportation (DOT). However, as the Government Accountability Office (GAO) and others have reported, there are barriers to planning and implementing intermodal projects. GAO's report examines (1) barriers that inhibit intermodal transportation; (2) actions DOT has taken to address these barriers and support Congress' goal; and (3) additional actions, if any, that DOT could take to better address barriers. GAO analyzed information from DOT and transportation experts and talked with transportation officials from various states and localities throughout the country. GAO recommends that the Secretary of Transportation direct one office or administration to lead and coordinate intermodal efforts at the federal level by improving collaboration and the availability of intermodal guidance and resources. DOT agreed to consider GAO's recommendation and provided technical comments that GAO incorporated, as appropriate.

Highlights: <http://www.gao.gov/highlights/d07718high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-718>

**13. July 20, Department of Transportation — DOT announces research grants.** The Department of Transportation's (DOT) Research and Innovative Technology Administration announced on Friday, July 20, the award of \$24.5 million for 20 U.S. universities to work with the Department to solve national and regional transportation challenges. The amounts awarded represent the current year's funding for each school, which previously received a four-year designation as a DOT-sponsored University Transportation Center. Universities receiving \$1.6 million from the Department are the Massachusetts Institute of Technology, the City University of New York, Pennsylvania State University, the University of Tennessee, Purdue University, Texas A&M University, the University of Nebraska-Lincoln, North Dakota State University, the University of California-Berkeley, and the University of Washington.

Source: <http://www.dot.gov/affairs/dot7107.htm>

**14. July 20, Associated Press — TSA: Airplane ban on lighters ends August 4.** Airline passengers will be allowed to bring most cigarette lighters on board again starting next month, freeing airport screeners to spend more time searching for explosives. And travelers without infants along will be allowed to carry more breast milk on planes to accommodate working mothers. Starting August 4, air travelers will be allowed to carry-on disposable butane lighters, such as Bics, and refillable lighters, like Zippo, the Transportation Security Administration (TSA) announced Friday, July 20. But torch-style lighters, which have hotter flames, will still be banned. "Explosives remain the most significant threat to aviation," said TSA administrator Kip Hawley. "By enabling our officers to focus on the greatest threats, we are using our officers' time and energy more effectively and increasing security for passengers." Lighters are the leading item seized at airport checkpoints, an average of more than 22,000 a day. It costs TSA \$4 million a year to dispose of them because they contain hazardous materials. The United States has been the only nation in the world to prohibit carry-on lighters, and last year Congress gave the TSA administrator discretion to drop the ban if he decided it was not enhancing aviation security.

For additional information: <http://www.tsa.gov/travelers/sop/index.shtm>

Source: [http://www.usatoday.com/travel/news/2007-07-20-airplane-lighters\\_N.htm](http://www.usatoday.com/travel/news/2007-07-20-airplane-lighters_N.htm)

**15. July 20, Washington Post — Virgin America ticket sales thwarted by cyber attack.** Virgin America, a new low-cost carrier scheduled to start service in Washington, DC, in the coming months, struggled to sell its first tickets yesterday after its Website was shut down or slowed to a crawl for most of the afternoon by a cyber attack, a company spokesperson said. "It's pretty clear that it was an absolute attempt to crash our site," said Gareth Edmondson-Jones, adding that he did not know who launched the attack. Edmondson-Jones called the incident an "SYN cyber attack." A SYN assault is a "denial of service attack" in which a herd of computers is directed to ask a Website for data but then, in effect, refuses to accept that information. When enough of these requests pile up, legitimate users can't get through to the site.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/19/AR2007071902343.html>

**16. July 20, Reuters — Airbus says Brazil jet approved to fly without reverser.** Debate over the cause of Brazil's worst air crash — on Tuesday, July 17, in Sao Paulo — has shifted from the slick runway to the aircraft's braking systems after it was disclosed one of the A320 airliner's thrust reversers was not operating at the time of the accident. Nearly 200 people were killed in the crash. "The A320 Master Minimum Equipment List approved by the certification authorities stipulates that the aircraft can fly for up to 10 days with a thrust reverser inoperative," said an Airbus spokesperson at its Toulouse, France, headquarters on Friday, July 20. Aviation experts say thrust reversers complement the brakes but are not the aircraft's primary braking system and that it is usually safe to fly without them. But the advantage to airlines and pilots is that they reduce wear on brakes and can shorten landing distances when needed. Brakes are among the costliest items to maintain. The lack of a reverser is not likely in itself enough to cause an accident without a series of other adverse factors, such as landing speed, the touchdown point, runway wetness, bad weather and other potential technical problems, said aviation consultant Pierre Condon.

Source: <http://www.usatoday.com/travel/flights/2007-07-20-Airbus-Bra>

[[Return to top](#)]

## **Postal and Shipping Sector**

**17. *July 20, WPTZ Plattsburgh (VT)* — Police: West Burke bomb scare was prank gone awry.**

The West Burke, VT, post office was evacuated Friday morning, July 20, after a customer brought what he believed to be an explosive device into the building. Police said a homeowner found a suspicious package in his mailbox and brought it to the post office. The postmaster immediately called police, put the device in a container, and evacuated the building. Hours later, the Vermont State Police explosives unit discovered the package actually contained a bottle filled with a household cleaner. Police said they believe someone tried to blow up the homeowner's mailbox, but didn't mix the chemicals right. Police said the ordeal cost \$8,000 in wasted resources but because the package was brought to a post office, federal investigators will now be involved, and that the person responsible could face prison and a \$500,000 fine.

Source: <http://www.wptz.com/news/13721768/detail.html>

[[Return to top](#)]

## **Agriculture Sector**

**18. *July 20, Stop Soybean Rust News* — Soybean rust found in five Texas counties.** Asian soybean rust was found in low levels in commercial soybean fields in five Dallas-area counties in northern Texas. This adds to recent finds in commercial fields in Austin, Fort Bend and Jackson counties reported Thursday, July 19. The new infected counties are Collin, Dallas, Ellis, Fannin and Hunt. This brings the total of Texas counties with soybean rust this year to 15, the highest count in the U.S. this year. Soybean rust has appeared in 42 counties and parishes in 2007, compared to only 25 in the U.S. and only one in Texas at this point last year.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=1066>

**19. *July 20, Michigan Ag Connection* — New invasive wood wasp found in Michigan.** An exotic wood wasp, *Sirex noctilio*, has made its way to Michigan, according to Deb McCullough, Michigan State University (MSU) forest entomologist. "The wasp was recently captured in a trap in Macomb County," McCullough says. "The larvae of this insect feed in stressed, dying or recently killed pine trees. *Sirex noctilio* has been an important pest in pine plantations in Australia, New Zealand and some South American countries." McCullough says the wood wasp is native to Europe, Asia and North Africa, but was discovered in New York in 2005 and in Ontario, Canada, in 2006.

Source: <http://www.michiganagconnection.com/story-state.php?Id=528&y r=2007>

**20. *July 20, Animal and Plant Health Inspection Service* — USDA updates testing regulations for U.S. cattle exports.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is amending its livestock exportation regulations to eliminate tuberculosis and brucellosis testing requirements for certain U.S. cattle prior to export. Under this final rule, APHIS is eliminating the requirement for pre-export tuberculosis and brucellosis

testing of certain cattle being exported to countries that do not require such testing. These actions relieve restrictions on certain exports of U.S. cattle to Canada for which testing is no longer necessary. Canadian animal health authorities have recognized U.S. success in eradicating brucellosis, tuberculosis and other diseases by establishing the Restricted Feeder Cattle Program, which allows certain untested feeder cattle to be imported into Canada. To participate in this program, the feeder cattle must originate from a state that has been designated by APHIS as brucellosis and tuberculosis free. In addition, should other countries importing U.S. cattle suspend or remove their testing requirements, this rule will ensure that U.S. cattle exporters receive the full benefits of no longer being required to perform pre-export tests. Currently all states are designated accredited-free for tuberculosis except Minnesota, Texas and portions of Michigan and New Mexico, and all states except Idaho and Texas are designated as class free for brucellosis.

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

21. *July 19, Associated Press* — **Citrus greening continues march across Florida.** A disease that kills trees and ruins fruit has moved into another of Florida's top citrus-producing counties, authorities said Wednesday, July 18. The discovery in Hardee County means citrus greening is now affecting trees in four of the top five production areas from last season. Those areas accounted for 60 percent of Florida citrus in 2005–06. Greening, first discovered in the state in September 2005, has now spread to two dozen citrus-producing counties, according to Florida Citrus Mutual, a grower-advocacy group. It has still not shown up in the top area, Polk County. Greening is spread by an insect, and can be active for two years before detection. Eventually the disease kills plants. Officials said greening probably arrived in Florida from infected Asian plant material. The Florida Department of Agriculture is holding grower-education meetings throughout Florida in coming weeks to share information about managing diseases.

Source: [http://www.orlandosentinel.com/business/orl-citrus1907jul19\\_0.7489469.story](http://www.orlandosentinel.com/business/orl-citrus1907jul19_0.7489469.story)

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

## **Food Sector**

22. *July 20, Reuters* — **China bans two food exporters amid pet food scare.** China has cancelled the business licenses of two firms that exported wheat protein tainted with toxic chemicals that wound up in pet food in the U.S., a senior quality control official said on Friday, July 20. U.S. consumers have been alarmed by a spate of pet deaths blamed on tainted wheat gluten and rice protein exported from China, as well as reports of toxins and disease in other Chinese exports. The two companies — Xuzhou Anying Biotechnology Development in Jiangsu province and Bingzhou Futian Biotechnology in Shandong province — "unlawfully added melamine in some of their protein products exported to the U.S.", quality watchdog chief Li Changjiang told a news conference.

Source: [http://www.reuters.com/article/healthNews/idUSPEK20317220070\\_720](http://www.reuters.com/article/healthNews/idUSPEK20317220070_720)

23. *July 19, Food Safety and Inspection Service* — **Georgia firm recalls canned meat products.** Castleberry's Food Company, an Augusta, GA, establishment owned by Bumble Bee Foods, LLC, is voluntarily recalling approximately 721,389 pounds of canned meat products that may contain *Clostridium botulinum* as a result of an equipment malfunction, the U.S. Department of Agriculture's Food Safety and Inspection Service announced Thursday, July 19. The canned

meat products were produced between April 30 and May 22, 2007 and were distributed to retail establishments in Alabama, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Indiana, Louisiana, Michigan, Mississippi, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Virginia, West Virginia and Wisconsin. The problem regarding the equipment malfunction was discovered during an investigation into illnesses in Indiana and Texas. The investigation led to a recall by the U.S. Food and Drug Administration of three types of meatless hotdog chili sauce. Botulism is a rare but serious paralytic illness caused by a nerve toxin.

Source: [http://www.fsis.usda.gov/News\\_ & Events/Recall\\_033\\_2007\\_Releas/index.asp](http://www.fsis.usda.gov/News_&_Events/Recall_033_2007_Releas/index.asp)

- 24. July 18, Agence France–Presse — Taiwan bans sales of U.S. pork.** Taiwan on Wednesday, July 18, banned sales of frozen pork imported from the U.S. after residues of a feed additive banned locally were found. Two shipments of U.S. pork totalling some 24 tons were detained by Customs in southern Kaohsiung city after they tested positive for clenbuterol, a feed additive designed to make animals leaner and more muscular, said a health official. Cheng Huei–wen, director of the Department of Health's Bureau of Food Sanitation, said the feed additive, approved in the U.S., Canada and some Asian countries but banned in the European Union, could cause palpitations only if taking in excessive amounts.

Source: [http://news.yahoo.com/s/afp/20070718/hl\\_afp/taiwanushealthfo  
od\\_070718171932;\\_ylt=AtHqn73eAK2kYKPCjxnQuuJOrgF](http://news.yahoo.com/s/afp/20070718/hl_afp/taiwanushealthfood_070718171932;_ylt=AtHqn73eAK2kYKPCjxnQuuJOrgF)

[[Return to top](#)]

## **Water Sector**

- 25. July 20, Associated Press — Four hurt in water plant explosion.** A chlorine explosion at a Colorado water treatment plant injured four people Friday, July 20, and heavily damaged the facility, authorities said. No water–quality problems were expected because other plants in the system were still operating, said Judy Dahl, business manager for the Little Thompson Water District. A truck was unloading chemicals at the filtration plant when the explosion happened, but it wasn't clear what set it off, Dahl said.

Source: <http://abcnews.go.com/US/wireStory?id=3398778>

[[Return to top](#)]

## **Public Health Sector**

- 26. July 21, Associated Press — Shortage of doctors affects rural U.S.** A national shortage of doctors is hitting poor places the hardest, and efforts to bring in foreign physicians to fill the gap are running into restrictions. Doctors recruited from places such as India, the Philippines and sub–Saharan Africa to work in underserved areas like the Mississippi Delta and the West already face an arduous and expensive gauntlet of agencies, professional tests and background checks to secure work papers and permanent residency. Those restrictions have only tightened in the years since 9–11, and now many believe the process will become more difficult after the attempted terrorist bombings in Britain that have been linked to foreign doctors. The government estimates that more than 35 million Americans live in underserved areas, and it

would take 16,000 doctors to immediately fill that need, according to the American Medical Association. And the gap is expected to widen dramatically over the next several years, reaching 24,000 in 2020 by one government estimate. A 2005 study in the journal Health Affairs said it could hit an astonishing 200,000 by then, based on a rising population and an aging work force. America's rural and inner-city poor already are suffering the most. Source: <http://www.foxnews.com/wires/2007Jul21/0.4670.DoctorDeficit.00.html>

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

## **Government Sector**

**27. *July 19, Information Week* — FBI analyst sentenced to 10 years for stealing national secrets.** A former U.S. Marine and FBI analyst was sentenced to 10 years in federal prison for espionage charges in connection with stealing classified national defense documents from the White House, the FBI, the Department of Defense, and the U.S. Department of State. Leandro Aragoncillo, 48, received his sentence on Wednesday, July 18, in U.S. District Court in Newark, NJ. Aragoncillo used text messages, Web-based e-mail accounts and database queries to pull off the espionage. But it was the same technology that helped the government track him down and build a case against him. The e-mails sent, the phone calls made, and the stolen information archived on a set of CDs all left a digital trail that was his ultimate undoing. Aragoncillo's case marks the first time in modern history that someone has been charged with spying out of the White House. The man who was a career Marine and had served under two vice presidents in the White House had pled guilty to stealing information in an attempt to foster a political coup in the Philippines, his home country. Source: <http://www.informationweek.com/news/showArticle.jhtml?articleID=201200012>

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

## **Emergency Services Sector**

**28. *July 20, Federal Computer Week* — First responders to get more credentials.** The Department of Homeland Security (DHS) is working on national standards for credentials for first responders, including private-sector emergency workers, but development is still in the early stages, according to congressional testimony July 19. The Federal Emergency Management Agency (FEMA) is establishing a working group for developing and integrating credentialing requirements and programs such as the First Responder Authentication Card and Common Credential projects. Marko Bourne, FEMA's director of policy and planning for analysis and evaluation, told the House Homeland Security Committee's Emergency Communications, Preparedness and Response Subcommittee. Those programs also are being coordinated with wider government credentialing efforts through the DHS Screening Coordination Office, Bourne said. DHS and FEMA are developing the first responder credentialing programs that include public safety, fire, police and medical responders, and private-sector emergency workers. DHS and FEMA are working on a national identification card system that can verify identities of responders who appear at an incident scene. They are also working to define categories of workers, such as firefighters, hazardous-materials teams and private-sector workers.

Source: <http://www.fcw.com/article103288-07-20-07-Web>

29. *July 20, Federal Emergency Management Agency* — **Statement by FEMA Administrator R. David Paulison regarding trailer air testing plans.** Over the last two months, the Federal Emergency Management Agency (FEMA) has significantly increased its focus on formaldehyde-related health concerns raised by Gulf Coast disaster victims. These individuals reside in FEMA-provided travel trailers and mobile homes in the Gulf States. Formaldehyde is a common indoor air pollutant that can be found in nearly all homes and buildings. It is a colorless gas that is released into the home from a variety of indoor sources. Formaldehyde can also be found in a variety of materials used in home construction and products for everyday living. FEMA has received a relatively small but meaningful number of inquiries from residents of FEMA trailers who have had medical symptoms possibly related to formaldehyde fumes. Today (Friday, July, 20), I am announcing several steps FEMA has taken to address these concerns and to work more closely with residents who may have concerns about formaldehyde exposure. These include: Air quality testing and research, additional outreach to travel trailer occupants, a dedicated toll-free help line, medical community outreach, and reinforcing FEMA's commitment to the public.

Source: <http://www.fema.gov/news/newsrelease.fema?id=38019>

30. *July 20, Boston Globe* — **Local emergency officials given access to DOT cameras on I-95.** Municipal police and fire departments in New Haven and Fairfield Counties in Connecticut will be given real-time access to images generated by state traffic cameras along Interstate 95, Governor M. Jodi Rell announced Friday, July 20. State Department of Transportation (DOT) officials met with local authorities who had been pushing for access to the images, and had threatened to oppose a \$40 million state plan to replace the cameras in an upgrade. "In any emergency, every minute is critical," Rell said in a news release. "Images from the scene give first responders the information they need to plan next steps and take the quickest possible action." About 100 cameras provide state police and the DOT with views of traffic jams, accidents and other highway problems and emergencies.

Source: [http://www.boston.com/news/local/connecticut/articles/2007/07/20/local\\_emergency\\_officials\\_given\\_access\\_to\\_dot\\_cameras\\_on\\_i\\_95/](http://www.boston.com/news/local/connecticut/articles/2007/07/20/local_emergency_officials_given_access_to_dot_cameras_on_i_95/)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

31. *July 20, VNUNet* — **'Critical' BitTorrent flaw hits Opera.** A "highly critical" vulnerability has been found in the Opera Web browser which could be exploited to remotely compromise a user's system. The flaw is caused when Opera uses already freed memory to parse BitTorrent headers, and can lead to an invalid object pointer being de-referenced. This can be exploited to execute arbitrary code if the user is tricked into clicking on a specially-crafted BitTorrent file and then removes it from the download pane by right-clicking. The vulnerability is reported in version 9.21 of Opera on Windows, but security monitoring Website Secunia, which rated the flaw "highly critical," said that other versions may also be affected. The problem can be fixed by upgrading to Opera 9.22.

Source: <http://www.vnunet.com/vnunet/news/2194683/highly-critical-bit-torrent-flaw>

32. *July 20, InformationWeek* — **Spammers exploiting new Simpson's movie.** Security researchers reported spotting a spam campaign that is preying on interest in the upcoming Simpson's movie. The spammed e-mails try to lure unsuspecting users to a Website, where their e-mail address will be harvested for later spamming attacks, according to researchers at Sophos. To get users to visit the site, the spam claims recipients will be given a \$500 Visa gift card if they click on a link and participate in an online survey about the movie. Each e-mail contains a graphic of Homer Simpson sitting on his sofa wearing a Superman crop-top and tighty-whities. A message in the image asks: "Will you go see the movie The Simpsons? Take our short survey now."

Source: [http://www.informationweek.com/security/showArticle.jhtml;jsessionid=OKODGNODVOEWEQSNDLPSKHSCJUNN2JVN?articleID=20120017\\_1](http://www.informationweek.com/security/showArticle.jhtml;jsessionid=OKODGNODVOEWEQSNDLPSKHSCJUNN2JVN?articleID=20120017_1)

33. *July 19, U.S. Computer Emergency Readiness Team* — **US-CERT Technical Cyber Security Alert TA07-200A: Oracle releases patches for multiple vulnerabilities.** Oracle has released patches to address numerous vulnerabilities in different Oracle products. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial-of-service. Systems Affected: Oracle Database; Oracle Application Server; Oracle Collaboration Suite; Oracle E-Business Suite and Applications; Oracle PeopleSoft Enterprise and JD EnterpriseOne. Solution: Apply the appropriate patches or upgrade as specified in the Critical Patch Update — July 2007. Note that this Critical Patch Update only lists newly corrected vulnerabilities. As noted in the update, some patches are cumulative, others are not. Oracle E-Business Suite and Applications patches are not cumulative, so E-Business Suite and Applications customers should refer to previous Critical Patch Updates to identify previous fixes they want to apply. Vulnerabilities described in the July 2007 CPU may affect Oracle Database 10g Express Edition (XE). According to Oracle, Oracle Database XE is based on the Oracle Database 10g Release 2 code. Known issues with Oracle patches are documented in the pre-installation notes and patch readme files. Please consult these documents and test before making changes to production systems.

Oracle Critical Patch Update: <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html>

Oracle Database 10g Express Edition (XE):

<http://www.oracle.com/technology/products/database/xe/index.html>

Source: <http://www.us-cert.gov/cas/techalerts/TA07-200A.html>

## 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

34. *July 21, CBS2 (NJ)* — **Jersey City woman finds missile launcher on lawn.** A Jersey City, NJ,

woman made what to her and her neighbors was a shocking discovery Friday morning, July 20, when she noticed a military rocket launcher lying in the grass. Niranjana Besai was leaving her house to go to work just after 8 a.m. EDT when she spotted the launcher on her front lawn. "I read it and it [said] 'missile,'" Besai told CBS 2 HD. "There was little 'missile' [writing] on it." Sources tell CBS 2 HD that the device is an AT-4 missile launcher that is used to fire against tanks and buildings. It was deemed inoperable and not a threat before it was turned over U.S. Army officials at the New Jersey's Fort Monmouth. Army officials tell CBS 2 HD that the launcher does have a serial number and they are in the process of tracing the weapon to see if it had been removed off base by Army personnel or if it was stolen. Officials initially expressed concern after discovering that Besai's house is located along a flight path for Newark Liberty International Airport. They later learned that used, inoperable AT-4 tubes are sold to the public through military surplus Websites and other outlets.

Source: [http://wcbstv.com/topstories/local\\_story\\_201113005.html](http://wcbstv.com/topstories/local_story_201113005.html)

**35. *July 20, Associated Press* — People trapped in St. Louis' Gateway Arch for two hours.**

About 200 people were trapped inside the 630-foot Gateway Arch for about two hours after an apparent power outage, authorities said. The power went out around 8:45 p.m. CDT Saturday night, July 21, stalling two trams filled with about 40 people each, Mike Maris, deputy superintendent of the Gateway Arch, told the St. Louis Post-Dispatch. About 100 other people were stranded at the top of the monument of stainless steel, Maris said. He said the evacuation of the south tram, where one of nine cables may have broken, took about two hours. Power eventually was restored to the north tram, and stranded visitors no longer had to use the stairs to evacuate, Capt. Steve Simpson, a spokesperson for the St. Louis Fire Department, told the newspaper. Simpson said rescue crews treated two people. One was given oxygen and the other was diabetic. Maris said the Arch would open Sunday with only the north tram running. The 630-foot-tall structure is operated by the National Park Service and opened in 1966. It is one of the region's most popular attractions.

Source: [http://hosted.ap.org/dynamic/stories/T/TRAPPED\\_IN\\_ARCH?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/T/TRAPPED_IN_ARCH?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT)

**36. *July 17, Dallas Morning News* — Plano police warn residents about bottle bombs.** After a loud knock and then explosion, Susan Bagen opened her front door to find a bubbling green liquid that smelled like acid covered her porch and door. Someone had left a "bottle bomb" at her house. The homemade bombs are made by combining a number of ingredients in a plastic bottle. After a matter of seconds, the bomb explodes. While the bombs may sound like a juvenile prank, Plano, TX, police said the devices can cause serious injury and issued this week a safety alert for residents. Plano police said such bombs have appeared in fields, parking lots and mail boxes for the past several years. There have been five such cases in the past five months, spokesperson Rick McDonald said. But investigators are taking this recent incident more seriously because it was Plano's first reported case where a bottle bomb was left on a porch when someone was home and there was the possible intent of hurting someone, Officer McDonald said. While the bombs may sound like a juvenile prank, Plano police said the devices can cause serious injury and issued this week a safety alert for residents.

Source: <http://www.dallasnews.com/sharedcontent/dws/news/city/collin/plano/stories/071807dnmetbottlebomb.846d4c76.html>

[[Return to top](#)]

## General Sector

37. *July 19, Associated Press* — **Blast shows age of U.S. infrastructure.** With a blast that made skyscrapers tremble, an 83-year-old steam pipe sent a powerful message that the miles of tubes, wires and iron beneath New York and other U.S. cities are getting older and could become dangerously unstable. The steam conduit that exploded beneath a Manhattan street at the height of rush hour Wednesday, July 17, just a block from Grand Central Terminal, was laid when Calvin Coolidge was president, and was part of a system that began providing energy to city buildings in 1882. Investigators are still trying to determine what caused the explosion, but some experts said the age of the city's infrastructure was a possible factor. From Boston to Los Angeles, a number of American cities are entering a middle age of sorts, and the infrastructure propping them up is showing signs of strain. Thousands of miles of underground water and sewage pipes are nearing the end of their expected life. Electrical systems, operating with components that are decades old, have been groaning to handle record power demand. The American Society of Civil Engineers estimates that it will take \$1.6 trillion over the next five years to get the nation's roads, bridges, dams, water systems, and airports into good condition. Source: [http://hosted.ap.org/dynamic/stories/M/MANHATTAN\\_EXPLOSION?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/M/MANHATTAN_EXPLOSION?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT)

[[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.