



Department of Homeland Security Daily Open Source Infrastructure Report for 31 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

- VNUNet reports the Department of Homeland Security has set out security requirements for automated control systems, principally in the power industry, to protect installations against physical and cyber-attacks. (See item [1](#))
- United Press International reports an incomplete job by a pest control contractor sparked an FBI terror investigation and forced the temporary shutdown of three of Washington, DC's Metro stations on Sunday, July 29. (See item [11](#))

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 30, VNUNet — Homeland Security warns on U.S. power threat.** The Department of Homeland Security (DHS) has set out security requirements for automated control systems, principally in the power industry, to protect installations against physical and cyber-attacks. Surprisingly for a document dealing with automated systems as opposed to data networks, it includes recommendations about protection against spam and social engineering, threats not normally associated with control systems. Security firm Verisign expressed fears in its most recent weekly iDefense security bulletin that "so many of the problems that some hoped would either never migrate from the IT world into the control system world (social engineering, spam,

etc) or be so rare as to be negligible, are apparently sufficient enough threats to be viewed as issues of concern for control systems." Many of the recommendations in the Catalog of Control System Requirements (draft) July 2007 (PDF) report describe basic cyber-security measures. These include installing antivirus software and ensuring that DNS is not used for control systems to protect against denial of service attacks. Other recommendations include not using VoIP, IM, FTP, HTTP and file sharing on control systems.

Source: <http://www.vnunet.com/vnunet/news/2195190/homeland-security-warns-power>

- 2. July 30, Institute for Energy and Environmental Research — Energy policy study points the way to U.S. energy future without fossil fuels or nuclear power.** A new study concludes that the U.S. could eliminate almost all of its carbon dioxide emissions by the year 2050 without the use of nuclear power. The study, Carbon-Free and Nuclear-Free: A Roadmap for U.S. Energy Policy, was produced by the Nuclear Policy Research Institute and the Institute for Energy and Environmental Research. The "Roadmap" concludes that the United States can achieve a zero-CO₂ economy without increasing the fraction of Gross Domestic Product devoted to lighting, heating, cooling, transportation, and all the other things for which we use energy. Net U.S. oil imports can be eliminated in about twenty-five years or less, the study estimated. According to the Roadmap, North Dakota, Texas, Kansas, South Dakota, Montana, and Nebraska each have wind energy potential greater than the electricity produced by all 103 U.S. commercial nuclear power plants. Solar energy is even more abundant — solar cells installed on rooftops and over parking lots can provide most of the U.S. electricity supply. Recent advances in lithium-ion batteries are likely to make plug-in hybrid cars economical in the next few years.

Executive Summary: <http://www.ieer.org/carbonfree>. The full study will be available for download in August 2007.

Source: <http://www.ieer.org/carbonfree/pressrelease.html>

- 3. July 30, Associated Press — Car crashes at nuclear weapons plant.** A driver ran a checkpoint at a nuclear weapons plant early Monday, July 30, and crashed into a barrier, then fled on foot, authorities said. Guards at the Y-12 nuclear weapons plant in Oak Ridge, TN, said the man "appeared to be impaired in some way" when they stopped him around 5 a.m. EDT at a security checkpoint near a rear entrance, spokesperson Bill Wilburn said. They asked him for identification, but the man hit the gas and drove through the checkpoint, then crashed into security barriers a short distance away, Wilburn said. "When he hit that, he jumped out of the car and ran away. He left the car there with the engine still running," Wilburn said. He said the guards told him the car had been hot-wired. No weapons were in the car. Oak Ridge police were searching for the driver. Steve Wyatt, spokesperson for the National Nuclear Security Administration, downplayed the crash, saying it was "next to nothing."

Source: http://hosted.ap.org/dynamic/stories/W/WEAPONS_PLANT_CRASH?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

- 4. July 29, Roanoke Times (VA) — To dismay of power utilities, coal emissions are under fire.** The emergence of global warming as a mainstream concern has altered the political landscape for coal. Just two months ago the Department of Energy issued a report highlighting coal's "resurgence" in electricity generation. But increasing worries about global warming caused by emissions from power plants, automobiles and other sources could pose a roadblock for the roughly 150 coal-fired power plants that have been proposed to satisfy rising electricity

demand. This month, Citigroup downgraded coal company stocks, citing the politics of global warming among other factors. Power companies are coal's largest customers, so new laws would make it more expensive to burn coal relative to other fuels, especially natural gas, and could have a major impact on the industry. Several states have taken steps to make it tougher to build conventional coal-fired plants, and there are multiple bills intended to curb carbon dioxide emissions circulating on Capitol Hill. Several technologies are in development to capture the carbon dioxide emitted by coal-fired power plants, but a solution on where to store the gas is not expected for a decade or more.

Source: <http://www.roanoke.com/news/nrv/wb/126136>

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

Chemical Industry and Hazardous Materials Sector

5. *July 30, Evansville Courier & Press (IN)* — **Leaking tanker prompts road closure.** A tanker truck loaded with 7,800 gallons of ethanol overturned on Old Henderson Road in Evansville, IN, and began leaking, creating a potentially hazardous situation. "The material is very flammable, if it found an ignition source," said Lt. Dennis Daniel of the Vanderburgh Sheriff's Office, explaining why officials requested a "safety zone" of one-half mile. According to emergency dispatches, the chemical was leaking at a rate of 50 gallons per minute. Old Henderson Road closed in both directions as crews cleaned up the site.

Source: <http://www.courierpress.com/news/2007/jul/30/overturned-semi-leaking-ethanol/>

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

Defense Industrial Base Sector

6. *July 27, Government Accountability Office* — **GAO-07-860: DoD Business Transformation: Lack of an Integrated Strategy Puts the Army's Asset Visibility System Investments at Risk (Report).** The Department of Defense (DoD) established a goal to achieve total asset visibility (TAV) over 30 years ago, but to date it has been unsuccessful. The Government Accountability Office (GAO) was requested to (1) determine whether the Army has a systems strategy for achieving TAV, (2) determine if the Army's business system investment governance structure is consistent with DoD guidance, and (3) evaluate the Army's effort to correct previously reported problems with the Logistics Modernization Program (LMP). GAO obtained an understanding of the Army's efforts to achieve TAV, oversee and manage its business system investments, and address previously reported LMP problems. GAO makes five recommendations to DoD and the Army: (1) develop a concept of operations for the Army; (2) develop policies, procedures, and processes to manage investments from a portfolio perspective; (3) establish an independent verification and validation function; (4) require that any future General Fund Enterprise Business System economic analysis is prepared in accordance with applicable policies; and (5) direct that LMP use an independent system test team. Overall, DoD concurred with the recommendations and stated that it will work diligently to close them.

Highlights: <http://www.gao.gov/highlights/d07860high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-860>

Banking and Finance Sector

7. *July 30, Techworld* — **New 'Glamour' Trojan demands ransom.** The two most prominent ransomware Trojans of recent times could be the work of the same people, or a related group of criminals, an analysis has suggested. Last week, a new ransomware Trojan appeared on the radar of security researchers, and was quickly identified as a modified version of the GpCode nasty that first hit the Internet as long ago as Spring 2005, and was tracked to a Russian site. As with its predecessors, the new Trojan, also named "Glamour," sets out to encrypt data files on any PC it infects, demanding a ransom of \$300 in return for a key to unlock files. Now an analysis from security research outfit Secure Science Corporation (SSC) has plotted the large number of similarities between the new GpCode and another version that appeared in 2006. Of the 168 functions identified in the code of the new variant, 63 were identical to the older 2006 version.

Source: http://www.infoworld.com/article/07/07/30/New-Trojan-demands-ransom_1.html

8. *July 28, eWeek* — **MySpace worm uses fast-flux to dodge detection.** A complex attack that in June was discovered to be turning MySpace.com users' sites into bots to serve phishing scams and viruses is just one example of fast-flux: a new way of hiding phishing and malware delivery sites behind ever-shifting networks of proxy servers that are next to impossible to track down, security experts have said. In late June, some MySpace user pages were seeded with malware designed to exploit one of three recently patched security holes in Windows and Internet Explorer. The exploit started with a Flash movie installed on multiple compromised MySpace pages that led users to a spoofed MySpace log-in page. That log-in page hosted a number of exploits that downloaded malware and tried to snatch visitors' MySpace credentials. Once the botnet commanders secured a MySpace user's credentials, they then updated the user's site to host malware. Old-school bot networks were set up with compromised machines at the beck and call of a command-and-control computer. Fast-flux networks, on the other hand, come with a new layer of abstraction. Now, machines are getting compromised and used merely as frontline proxies, with the botnet commanders safely tucked away behind a veil of constantly shifting IP addresses.

Source: <http://www.eweek.com/article2/0.1895.2163609.00.asp>

9. *July 27, Business Day (South Africa)* — **Money laundering fight costs banks.** The cost of fighting money laundering has risen dramatically for banks across the world due to the increasing complexity of the financial markets in which they operate, according to a new report released by KPMG Forensic Thursday, July 26. KPMG's study, which included 224 banks from 55 countries, found that spending by financial institutions on anti-money-laundering systems and processes had risen by an average of 58 percent over the past three years. In the U.S., the Middle East and Africa, spending had increased 70 percent or more. These increases are far in excess of banks' own predictions when KPMG Forensic carried out its last study in 2004, when respondents on average predicted an increase of 43 percent. The biggest spending is on the monitoring of transactions and costs of training staff. However, there is still a significant concern among banks that governmental and international regulation needs to be more effectively targeted. Half of the banks that took part in the study said that, while they

believed that the overall regulatory burden was acceptable, the requirements needed to be better focused.

Source: http://www.businessday.co.za/articles/economy.aspx?ID=BD4A52_5759

10. *July 26, InfoWorld* — **IT pros fear iPod data theft.** A new study published by Credant found that 67 percent of the 323 IT workers surveyed consider the iPod to be a potential data security risk. However, short of some sort of major disaster that links the Apple devices to data leakage, 49 percent of those surveyed said they likely wouldn't do anything new to protect against misuse of the gadgets. Some 46 percent said that their companies have already established policies dictating acceptable use of the media players. Truthfully, the Credant survey highlights the continued disregard among companies in dictating the use of USB-capable storage devices in general, of which the iPod is clearly just one of the most popular. When asked to rank which USB devices they considered to be most dangerous in terms of potential corporate data loss, a vast majority (86 percent) of respondents still ranked traditional handheld storage drives, and SD-card carrying smartphones (13 percent) ahead of the iPod (10 percent).

Source: http://weblog.infoworld.com/zeroday/archives/2007/07/it_pros_fear_ip.html

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

Transportation and Border Security Sector

11. *July 30, United Press International* — **Dead birds cause Metro shutdowns.** An incomplete job by a pest control contractor sparked an FBI terror investigation and forced the temporary shutdown of three of Washington, DC's Metro stations on Sunday, July 29. Dozens of dead birds, most of them sparrows and starlings, were discovered Sunday at six Metro stations. As sightings of dead birds increased, officials from the FBI's joint terrorism task force and the National Institutes of Health launched an investigation. Metro spokesperson Cathy Asato said that a contractor hired by Metro to deal with pigeons did his job on a Sunday. The contractor spread poison at the stations but failed to remove the dead birds that ingested it.

Source: http://www.upi.com/NewsTrack/Top_News/2007/07/30/dead_birds_cause_transit_shutdowns/5102/

12. *July 30, Associated Press* — **Maine airport blames hubs for its delays.** Maine's Portland International Jetport is getting lumped together with a couple of the nation's largest airports: Chicago's O'Hare and New York's John F. Kennedy – for congestions and delays. From the beginning of the year through May, Portland had the nation's third-worst record for on-time arrivals, with 42 percent of flights arriving late by 15 minutes or more, according to government statistics. Only O'Hare and Kennedy were worse. Likewise, more than a third of departures from Portland were delayed. Portland also had more than double the national airport average of canceled flights. City Transportation Director Jeff Monroe said the problems begin at major hub airports and ripple through smaller airports like Portland. But Monroe acknowledged some flights have been held up for passengers going through security screening. The airport has struggled to reduce lines at security checkpoints, especially in the mornings when 18 flights leave between 6 a.m. and 7 a.m. EDT. Portland's poor figures also reflect increasingly congested skies, particularly in the Northeast, Monroe said. The Portland airport needs more gates and terminal space at the airport to move passengers and planes efficiently.

Source: http://www.usatoday.com/travel/flights/2007-07-30-portland-hub-delays_N.htm

13. *July 30, Department of Transportation* — **Denver's East Corridor and Gold Line Corridor projects selected to participate in Transportation's public-private partnership program.** Department of Transportation Secretary Mary E. Peters on Monday, July 30, announced two Denver rail projects will take part in a Department of Transportation pilot program to evaluate the benefits of forming public-private partnerships for federally-funded transit construction projects. The East Corridor extends 23.6 miles from Denver Union Station (DUS) in downtown Denver to Denver International Airport (DIA), and connects DUS and DIA with existing residential, commercial, and industrial areas. DUS is the central hub of the multi-modal network proposed in Regional Transportation District's FasTracks regional rail system. The Gold Line, a proposed 11.2-mile rail transit corridor, will begin at DUS, passing through Northwest Denver. Upon completion there will be six park-n-ride facilities and 2,050 new parking spaces. Construction on both the East and Gold Line Corridors is scheduled to begin in 2011. Unlike conventional procurement methods for new construction, in which specific jobs are bid out separately, public-private partnerships transfer responsibility for performing construction and operating responsibilities to a single private entity or a consortium of private companies.
Source: <http://www.dot.gov/affairs/fta1107.htm>
14. *July 30, Associated Press* — **Louisiana: Vessel hits pipeline, spills oil.** A vessel apparently struck a pipeline in the Gulf of Mexico on Sunday, July 29, leaving behind an 80-barrel oil spill that spread out into about two miles by eight miles in size, the Coast Guard said. By Monday morning the oil had dissipated in the hot and humid conditions, said Lt. Cmdr. Cheri Ben-Iesau, a senior investigating officer. The spill was located about eight miles from the east bank of Plaquemines Parish. The Coast Guard said authorities believed an unidentified vessel struck the pipeline, which was linked with an offshore well. The Coast Guard said the well was owned by Houston-based Bois d' Arc. The leak was stopped about 12:45 p.m. CDT on Sunday after apparently beginning sometime during the night, the Coast Guard said.
Source: <http://www.forbes.com/feeds/ap/2007/07/30/ap3966983.html>
15. *July 30, RFID Journal* — **Washington Driver's Licenses to Carry EPC Gen 2 Inlays.** Washington State's Department of Licensing has decided to deploy a technology trial of an RFID (Radio Frequency Identification)-enabled driver's license. The agency says it will work with a Beaverton, OR, provider of personal identification systems for government and commercial applications, to implement the pilot. In March of this year, Washington governor Christine Gregoire authorized the department to design the specialized driver's license for border crossings between the state and Canada. In addition to having an RFID inlay, the license (which will be called an Identocard) will also possess a digital watermark and other authenticators, and will give Washingtonians an alternative to carrying U.S. passports at land border crossings between Canada and Washington. The Department of Homeland Security has pre-approved the use of the RFID-enabled Washington State driver's licenses as an alternative to showing a U.S. passport or PASS card at border crossings between Washington and Canada, as long as the cards carry passive UHF EPC Gen 2 inlays, which the department has selected for the PASS cards it plans to issue for land border crossings. This will allow the Identocards to be readable by the same interrogators as those that will be used to read PASS cards.
Source: <http://www.rfidjournal.com/article/articleview/3514/1/1/>

16. July 30, *CBC News (Canada)* — First armed border officers stand on guard for Canada.

When people arrive at a Canadian border point from now on, the person inquiring what you purchased out of the country may — or may not — be toting a 9–mm semiautomatic pistol. As Canada's first few armed border officers went on duty, the government wasn't saying exactly where they would be posted. But Marie–Claire Coupal, a Customs Excise Union national vice–president based in Windsor, confirmed that the Windsor–Sarnia area, where bridges, tunnels and ferries link Ontario and Michigan, would have 11 armed officers on duty Monday, July 30. They were among 39 officers who graduated from weapons courses in Ottawa and Chilliwack, BC, on Friday, and are now authorized to carry handguns. That number is to grow to 4,800 over 10 years under a training and equipment program budgeted at \$101 million in its first two years. The 39 have been issued the government's chosen weapon, the Beretta Px4 Storm, a futuristic–looking Italian handgun with a plastic frame and a 17–round magazine. Until now, all Canadian border officers went unarmed, in contrast to their U.S. counterparts.

Source: <http://www.cbc.ca/canada/story/2007/07/30/armed-border.html>

17. July 29, *ABC News* — Pilot no–shows ground 200 Northwest flights.

Hundreds of passengers experienced disruptions in their travel plans this past weekend when Northwest Airlines canceled more than 200 flights. During a summer season already filled with record delays and cancellations, the nation's fifth–largest carrier cited pilot absenteeism for the problems. The pilots have said they were not playing hooky. They said their contract with Northwest limits their flying time to 90 hours per month and during this year's busy travel season their time sheets are maxed–out. This weekend's cancellations happened despite efforts by Northwest earlier this month to thin out its schedule so pilots would have enough hours. The union said the airline simply needs more pilots.

Source: <http://www.abcnews.go.com/GMA/Travel/story?id=3425531&page=1>

18. July 29, *CP News (Canada)* — Thousands stuck as BC Ferries cancels 21 sailings due to bomb threat.

Thousands of summer travelers were stuck for several hours Saturday, July 28, when BC Ferries was forced to cancel sailings after receiving a bomb threat that police considered credible. David Hahn, chief operating officer of BC Ferries, said the threat came in a 911 call to police at about 3:30 (local time) in the afternoon from a mall in suburban Coquitlam from a man with a Middle Eastern accent. Twenty–one sailings were cancelled and travelers were forced to wait in terminals near Vancouver, Victoria, and Nanaimo. Police and three sniffer dogs searched the ships, cars, campers, and buses and no one was allowed to leave the terminal until their vehicle had been inspected, said Hahn. One ferry had already left the terminal and had to be turned back. As well, all the vehicles clogging the parking lot at the Tsawwassen terminal a 40–minute drive south of Vancouver had to be searched. Once inspected, the owners were asked to leave. The big ships between Tsawwassen and Schwartz Bay carry up to 470 cars and 2,100 passengers. In the summer, ferries depart between the two terminals every hour.

Source: http://www.securenet.bc.ca/NewsCentral/News_Library/News_Releases/nl072807.htm

19. July 27, *Department of Transportation* — FRA grant supports wireless communications research for PTC application.

The Federal Railroad Administration (FRA) issued a \$4,465,000 grant to the Railroad Research Foundation to continue development and testing of wireless communications devices and systems for use with Communications Based Train Control (CBTC) technology. CBTC is a form of Positive Train Control (PTC) that can

automatically control train movements and speed to enhance safety when the locomotive engineer fails to take appropriate action. In addition to advancing technical developments, a primary aim of this grant funding is to design and build a Universal Onboard Platform that will allow a locomotive to easily switch between different PTC operating systems, or to another onboard signaling system, when it travels from one railroad network to another.

Source: <http://www.dot.gov/affairs/dot7307.htm>

[[Return to top](#)]

Postal and Shipping Sector

20. *July 29, Kingman Daily Miner (AZ)* — **Bomb destroys postal box.** An explosive device destroyed a U.S. postal box early Friday morning, July 27, in Kingman, AZ. A \$500 reward is being offered for information identifying the person or persons involved with the incident. At about 4 a.m. MST, Mohave County Sheriff's deputies responded to the corner of Northern Avenue and N. Arizona Street in Kingman where a postal box was on fire due to a detonated device. Hualapai Fire Department personnel also responded and extinguished the fire. All of the mail inside the postal box was destroyed.

Source: <http://www.kingmandailyminer.com/main.asp?SectionID=13&SubSectionID=18&ArticleID=12745>

[[Return to top](#)]

Agriculture Sector

21. *July 29, Palm Beach Post (FL)* — **Mite wreaks havoc on palms.** Marjorie Hoy saw them in April, on the Caribbean island nation of Dominica. Hundreds of thousands of tiny, bright red creatures that seemed to be on each palm tree, banana, plantain and ginger plant in sight. Hoy, an entomologist at the University of Florida, was looking at a pest that for the past three years has been steadily making its way across the Caribbean to Florida. The red palm mite attacks 32 varieties of palms, as well as bananas and plantains, heliconias and even flowers such as the bird of paradise. An infestation of the mite in Florida could deal a heavy blow to the state's three billion dollar wholesale nursery business, seven percent of which is devoted solely to palms. The arachnid's effect also could be felt at the market, should the mite destroy enough banana plants and weaken a sufficient number of coconut palms. The mite already has made it to South Florida at least four times. Since April, it's been intercepted and destroyed at the seaports in West Palm Beach, Fort Lauderdale and Miami. Detected in India in 1924, the mite was first reported in the Western Hemisphere in Martinique in 2004, and has since spread to nine more countries.

Source: http://www.palmbeachpost.com/localnews/content/local_news/epaper/2007/07/29/m1a_RED_PALM_MITE_0729.html

22. *July 28, New York Times* — **House passes farm bill.** House Democrats voted on Friday, July 27, to approve a farm bill that would continue generous farmers' subsidies. The bill passed, 231 to 191, with 19 Republicans joining 212 Democrats in favor. The bill, is projected to cost about \$286 billion over five years. The House vote sets the stage for complicated negotiations when

the Senate takes up its version of the farm bill in the fall. In addition to a veto threat by the White House, the World Trade Organization is expected to rule on complaints by countries like Brazil and Canada that the subsidies violate free trade agreements. In an interim report this week, the WTO ruled that the U.S. had failed to change cotton subsidies, allowed under the previous farm bill, enough to conform to global trade rules.

Source: http://www.nytimes.com/2007/07/28/us/28farm.html?_r=2&ref=us&oref=slogin&oref=slogin

23. July 26, *Lahontan Valley News (NV)* — New state regulations aim to curb trichomonosis.

Trichomonosis is a sexually transmitted disease passed from bulls to cows. The disease induces abortions in pregnant cows. New trichomonosis regulations took effect July 1, in Nevada, in an effort to cut down on the number of calves lost due to the disease. The new regulations, handed down from the Nevada Department of Agriculture, require testing of bulls older than eight months prior to sale or coming into the state, unless the animals are being sold directly for slaughter.

Source: http://www.lahontanvalleynews.com/article/20070726/News/1072_60050

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

Food Sector

24. July 29, *Columbus Dispatch (OH)* — Fears over food safety on the rise. A recent survey indicates that 50 percent of U.S. consumers are more concerned about food safety than they were two years ago. In the survey, conducted online by Harris Interactive on behalf of IBM's Institute for Business Value, two of every five who answered said that they buy brands based on safety. And 70 percent of those surveyed said they don't trust the environmental and health claims of branded food products. Consumer confidence has slid since recalls of several foods, including peanut butter, lettuce, spinach and vegetable snacks, along with several imports from China, including toothpaste. The U.S. Department of Agriculture says that a quarter of all fruits, half of all nuts and two-thirds of the fish and shellfish consumed in the U.S. are imported. Food importers must be registered with the U.S. Food and Drug Administration, but fewer of their shipments are being inspected, the Government Accountability Office says. For example, inspection rates fell about 18 percent in Boston, 12.7 percent in Miami and 21.4 percent in San Francisco between 2003 and 2006, the agency says.

Source: http://www.columbusdispatch.com/dispatch/content/business/stories/2007/07/29/CONSUMER_FEARS.ART_ART_07-29-07_A1_LG7D9H7.html

25. July 27, *U.S. Food and Drug Administration* — California Department of Public Health announces botulism case. Mark Horton, director of the California Department of Public Health (CDPH), Friday, July 27, announced that a 51-year-old San Diego County woman has a confirmed case of botulism, a rare illness. The San Diego County Health and Human Services Agency and CDPH are investigating whether the woman's illness is associated with Castleberry Food canned products that were recently recalled due to possible contamination with the toxin that causes botulism. The woman reported purchasing and eating one of the products, Kroger Chili with Beans, prior to her illness in early July. Certain lots of Kroger Chili with Beans, in addition to a number of canned products under different brand names, were voluntarily recalled by Castleberry Food Co. of Augusta, GA, last week. The recall followed reports of four

illnesses of botulism in two states associated with the consumption of Castleberry Hot Dog Chili Sauce. The Kroger Chili with Beans product consumed by the San Diego County woman was thrown away before tests could be performed to determine if it was the definitive cause of the botulism.

Source: http://www.fda.gov/oc/po/firmrecalls/cdph07_07.html

26. *July 27, Associated Press* — **Japan's U.S. beef imports remain low.** A year after the lifting of Japan's latest ban on U.S. beef over mad cow concerns, imports of the meat remain far below the levels seen before the first ban was imposed in 2003, an official said Friday, July 27. The American beef industry was exporting 20,000 tons of beef per month to Japan before the meat was first banned in December 2003, according to the U.S. Meat Export Foundation. For the ten-month period from August 2006 through May 2007, Japan imported a total of 15,205 tons of U.S. beef, Agriculture Ministry official Mayuko Nishibori said. The period was the most recent one for which statistics are available, she added. U.S. beef imports have been gradually increasing in recent months, with 2,193 tons of the product having been imported in May alone, she said.

Source: <http://www.forbes.com/feeds/ap/2007/07/27/ap3961155.html>

[[Return to top](#)]

Water Sector

27. *July 29, Associated Press* — **Chinese police, protesters clash over contamination of drinking water.** Police clashed with thousands of villagers who protested after a brewery polluted local water supplies, a human rights groups said Sunday, July 29. It said seven protesters were detained and 20 injured. The paramilitary People's Armed Police moved in Friday, July 27, to break up the protest in Yuanshi, a town in the southwestern province of Sichuan, according to the Hong Kong-based Information Center for Human Rights and Democracy. Villagers protested after China Resources (Shifang) Breweries Co. dumped waste water, contaminating supplies used for drinking and farm irrigation, the center said. The incident came amid a string of protests in areas throughout China over pollution of farmland and water supplies by factories, chemical plants and other industrial projects.

Source: <http://news.bostonherald.com/international/asiaPacific/view.bg?articleid=1014029>
<http://news.bostonherald.com/international/asiaPacific/view.bg?articleid=1014029>

28. *July 28, Associated Press* — **Mine spill cuts water supply in China.** Mine runoff spilled into a central Chinese river, temporarily cutting off drinking water to more than 200,000 people, a state news agency reported. The runoff from a lead-zinc mine polluted the Zijiang River in Hunan province on Thursday, July 26, cutting off supplies to the riverside city of Lengshuijiang and residents downstream. It was reported that more than 39,000 cubic yards of lead-zinc residue were washed into the river after a drain collapsed at the private Zhongtai Mining Corp.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/28/AR2007072800596.html>

[[Return to top](#)]

Public Health Sector

29. *July 28, Reuters* — **South Africa tests first new TB vaccine in 80 years.** The first new vaccine against tuberculosis (TB) in more than 80 years has entered mid-stage trials in South Africa, where the killer disease is rife, scientists said on Saturday, July 28. If the tests are successful, a new shot against *M. tuberculosis* (TB) bacteria could be available within eight years. The vaccine was developed by researchers at Oxford University, who are now studying it in Phase II studies in the Western Cape. Despite widespread vaccination, one in 100 infants in the Western Cape suffers from TB disease, underscoring the need for better prevention. The current standard vaccine for TB is Bacille Calmette–Guerin, or BCG, which provides some protection against severe forms of the disease in children but is unreliable against pulmonary TB, the most common type.

Source: http://uk.reuters.com/article/healthNews/idUKL27834498200707_27

30. *July 28, Dallas Morning News* — **A&M lab employee lacked clearance in bioagent case.** At least one Texas A&M University lab employee exposed to a dangerous infectious agent last year didn't have federal approval to work with it, according to records reviewed by The Dallas Morning News. This revelation is the latest in a mounting scandal at A&M, stemming from the university's failure to report to the federal government one illness and several other cases of workers being exposed to "select agents." The U.S. Centers for Disease Control and Prevention has so far suspended the federally funded biodefense program's prize research and jeopardized its future. Nineteen federal investigators left College Station on Thursday, July 26, after four days examining a *Brucella* infection and several Q-fever exposures in campus labs.

Source: http://www.dallasnews.com/sharedcontent/dws/news/texasouthwest/stories/DN-a&mlab_28tex.ART.North.Edition1.41eaba7.html

31. *July 28, Reuters* — **Chicken smugglers caught in northeast's bird flu zone.** More than a dozen poultry farmers in India's bird flu-hit northeast have been caught trying to smuggle flocks of chickens out of the quarantine zone, police said on Saturday, July 28. Local residents were helping police stop people sneaking chickens and poultry products out from within a five km radius of a small farm at Chingmeirong village in Manipur state, the site of India's latest bird flu outbreak this week. There are no suspected human cases in India at the moment, state health officials said. A lab in the western city of Pune is testing blood samples taken from workers on the affected farm. Health workers have already killed around 25,000 chickens and destroyed thousands more eggs since Thursday to try and contain the virus. They plan to cull 150,000 in all within the quarantine zone by next week.

Source: http://in.reuters.com/article/topNews/idINIndia-286987200707_28

32. *July 27, Computerworld* — **Semantic Web helps protect public health.** Health officials and the U.S. government have become interested in ways of identifying bioterror incidents early to react and contain them, said Parsa Mirhaji, the director of the Center for Biosecurity and Public Health Information Research at the University of Texas, Houston. The problem was almost too much data. "We have information from hospital emergency departments, community clinics, pharmacy sales, laboratories, environmental safety commissions, pollution exposure in air and water," Mirhaji said. This is complex data, and to do any good it needs to be analyzed quickly — for normal patterns to provide a basis for comparison and for deviations from those patterns that might indicate a disease outbreak or a bioterror incident. This data comes from multiple

sources and systems that use different, often incompatible schema. Conventional analysis methods simply are not as effective — in an outbreak. To solve that problem, Mirhaji's team turned to Semantic Web technology. Semantic Web refers to the web of meaning and connectivity in large and complex data sets accessible from a distributed network. It's a way to organize complex data in meaningful ways by assigning a formal meaning to each element of data. This makes all data explicit, unambiguous and its interpretation identical for both machines and humans.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9028179&taxonomyId=16&intsrc=kc_top

- 33. July 26, *United Press International* — Infectious disease digital library planned.** The U.S. National Library of Medicine said a digital library to help in infectious diseases education will be developed under a \$413,087 grant. The money will be used by the University of Texas at Austin's School of Information, in collaboration with Massachusetts General Hospital and Harvard University, to create a digital library called "eMicrobes." It will be designed to assist healthcare professionals in identifying and treating the growing number of infectious diseases and global threats such as AIDS, tuberculosis, malaria and bio-terror, officials said. A team of physicians, medical librarians and medical education specialists will develop the library of interactive case studies and images.

Source: http://www.upi.com/NewsTrack/Science/2007/07/26/infectious_disease_digital_library_planned/4916/

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

Government Sector

Nothing to report.

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

Emergency Services Sector

- 34. July 29, *Dallas Morning News* — A&M program gives firefighters real-world training.**

About 40,000 emergency responders come to Texas A&M University's 120-acre training center annually for fire, rescue and hazardous-materials training. The Brayton Fire Training Field has 22 props that produce real flames, including pumps, a rail car rack, a loading terminal, and a liquefied natural gas plant that can simulate a variety of fires. It even has a hay-filled airplane fuselage and ship for rescuers to practice putting out flames in smoky conditions. Experts say that of the hundreds of facilities nationwide that offer live-fire training, the A&M center is one of the best at preparing firefighters for chemical plant explosions. Technology is changing the training, too. When the risk of lightning forces his class on emergency rescue indoors, instructor James Hyles puts Google Earth maps of the facilities where the students work on a big screen and has them identify vulnerabilities. "Looking at the big picture helps first responders devise good action plans," Hyles said. "They'll draw to a close proximity how they'd get someone out at their individual plant."

Source: <http://www.dallasnews.com/sharedcontent/dws/news/texasouthwest/stories/073007firetrain.36a875e.html>

35. July 21, *Houston Chronicle* — Texas bolsters role of retail giants in hurricane preparedness. Texas emergency officials are cultivating direct relationships with area retailers to respond quickly to disaster situations. As reported by the Houston Chronicle's Terri Langford, the state's new strategy is to combine government's network of local emergency responders and powerful communications tools with retailers' flexible and timely delivery systems. Retailers will train alongside government officials. All retailers are welcome to volunteer their assistance, and many have, including such giants as Wal-Mart and Home Depot. While some have expressed concerns that retailers might stand to profit from helping to plan disaster relief, retailers and government insist there is no hidden agenda, that no promises are made or contracts struck before a disaster, and that everyone stands to gain from working together. Communities get help swiftly, retailers hang onto their customers, and public services endure less strain. Texas Homeland Security Director Steve McCraw told the Chronicle that the new collaboration has already proved effective. Retailers responded quickly and effectively in such disasters as the tornado that struck Eagle Pass last April and in the severe flooding in several Texas counties.

Source: <http://www.chron.com/disp/story.mpl/editorial/4987284.html>

36. June 29, *Government Accountability Office* — GAO-07-854: Emergency Management Assistance Compact: Enhancing EMAC's Collaborative and Administrative Capacity Should Improve National Disaster Response. The Emergency Management Assistance Compact (EMAC) is a collaborative arrangement among member states that provides a legal framework for requesting resources. Working alongside federal players, including the Federal Emergency Management Agency and the National Guard Bureau, EMAC members deployed an unprecedented level of assistance in response to hurricanes Katrina and Rita. Although EMAC played a critical role in our nation's response to these hurricanes, the magnitude of these events revealed limitations. The Government Accountability Office (GAO) was asked to (1) examine how the use of EMAC has changed since its inception; (2) assess how well existing policies, procedures, and practices facilitate collaboration; and (3) evaluate the adequacy of the EMAC network's administrative capacity to achieve its mission. GAO examined documents and interviewed officials from 45 federal, state, and local agencies and offices. GAO makes recommendations to the Secretaries of the Department of Homeland Security and the Department of Defense to further enhance the administrative capacity required to support the EMAC network and to develop guidance and to formalize certain procedures to alleviate burdens experienced by EMAC members during catastrophic disasters.

Highlights: <http://www.gao.gov/highlights/d07854high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-854>

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

Information Technology and Telecommunications Sector

37. July 30, *eWeek* — Core Security to reveal new database attack vector. Researchers at Core Security Technologies have donned their black hats and are preparing a presentation about a new database attack vector that relies solely on the inherent characteristics of the indexing algorithms. The attack, which will be demonstrated Wednesday, August 1, against the MySQL database engine at Black Hat USA in Las Vegas, affects database management systems using

BTREE, the popular database indexing algorithm and data structure. Traditionally, database security breaches are mostly due to the abuse of wrongly configured authorization and actual control permissions or the exploitation of bugs in front-end Web applications through SQL injection, said Core Security Chief Technology Officer Ivan Arce. The presentation will involve the use of timing attacks, a common technique for breaking cipher system implementations, on database engines. Researchers from CoreLabs will explain how this technique can be used to extract information from a database by performing record insertion operations, which are typically available to all database users – including anonymous users of front-end Web applications.

Source: <http://www.eweek.com/article2/0,1895,2164067,00.asp>

38. July 30, *InformationWeek* — Verizon Wireless to acquire Rural Cellular for \$2.67 billion.

Verizon Wireless said it will acquire Rural Cellular Corporation for about \$2.67 billion in the latest example of the new attractiveness of rural wireless services. Announced Monday, July 30, Verizon Wireless said the acquisition will increase its customer base by more than 700,000. Rural Cellular's networks range across areas in Maine, Vermont, New Hampshire, New York, Massachusetts, Alabama, Mississippi, Minnesota, North Dakota, South Dakota, Wisconsin, Kansas, Idaho, Washington, and Oregon. While the thought of acquiring small rural wireless providers would have been shunned not too long ago, the transactions are becoming a way for major mobile phone service providers to grow their subscriber rolls.

Source: http://www.informationweek.com/management/showArticle.jhtml;jsessionid=VJPIV3BK13WSSQSNLRCCKHOCJUNN2JVN?articleID=201201_813

39. July 30, *Sophos* — Virus plays on Nintendo Mario game nostalgia.

IT security and control firm Sophos is warning of a new mass-mailing worm that is capitalizing on users' enthusiasm for Nintendo's iconic character, Mario. Once they open the e-mail, recipients are requested to click on an attachment that promises to run one of the classic Super Mario Bros games. E-mails sent by the worm use the following text in the message body: "Hi There, Do You Like Mario Bros ? Test it, and you'll like it ;] !" Attached to the e-mails is a file containing the Romario-A worm, which in addition to launching a game starring the portly Italian plumber, also attempts to infect other unprotected computers via mass-mailing itself as a file attachment, as well as spreading via removable shared drives. Sophos experts note that Romario-A aims to cause maximum impact by scheduling a daily task to ensure the worm runs regularly at a specified time.

Source: <http://www.sophos.com/pressoffice/news/articles/2007/07/mario.html>

40. July 28, *Los Angeles Times* — Three voting systems faulted.

Three of California's electronic voting systems — including those used in Orange, Riverside, San Bernardino and Ventura counties — can be easily hacked into, potentially compromising millions of votes, according to a detailed review announced Friday, July 27. Makers of Los Angeles County's InkaVote system did not submit its equipment in time, so it wasn't included, said Secretary of State Debra Bowen, who requested the study. The three systems evaluated, used by more than two-thirds of California's counties, also had problems with accessibility requirements for disabled and non-English-speaking voters. The findings of what some believe to be one of the most comprehensive electronic voting studies to date come as California registrars rush to prepare for the state's presidential primary election February 5. Over two months, dozens of experts in information technology organized by the University of California tested machines made by

Diebold Election Systems, Hart InterCivic and Sequoia Voting Systems. The analysts tried to infiltrate the three systems physically and electronically, without the safeguards that voting machine vendors or counties might use. "Under these conditions, the technology and security of all three systems could be compromised," the review said.

Report: http://www.sos.ca.gov/elections/elections_vsr.htm

Source: <http://www.latimes.com/news/local/la-me-vote28jul28.0.1784391.story?coll=la-home-center>

41. *July 27, IDG News Service* — **Hotmail maintenance glitch locks users out.** Microsoft's Windows Live Hotmail Webmail service remained inaccessible to a portion of its users for several hours on Friday, July 27, but the problem has been resolved. Windows Live Hotmail, which has about 310 million active users worldwide, became unavailable between approximately 6:30 a.m. U.S. Pacific Time and "late morning," a spokesperson for Microsoft said. She declined to specify how many users were affected, saying only that the problem affected "a limited set of customers." The problem, which erupted during maintenance work for Windows Live Hotmail, didn't lead to any loss of data for users, according to the spokesperson. Source: http://www.infoworld.com/article/07/07/27/Hotmail-maintenanc-e-glitch-locks-users-out_1.html

42. *July 27, Government Accountability Office* — **GAO-07-837: Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses (Report).** For many years, the Government Accountability Office (GAO) has reported that weaknesses in information security are a widespread problem with potentially devastating consequences — such as intrusions by malicious users, compromised networks, and the theft of personally identifiable information — and has identified information security as a governmentwide high-risk issue. Concerned by reports of significant vulnerabilities in federal computer systems, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the information security program, evaluation, and reporting requirements for federal agencies. As required by FISMA to report periodically to Congress, in this report GAO discusses the adequacy and effectiveness of agencies' information security policies and practices and agencies' implementation of FISMA requirements. To address these objectives, GAO analyzed agency, inspectors general, Office of Management and Budget (OMB), congressional, and GAO reports on information security. GAO is recommending that OMB strengthen FISMA reporting metrics. OMB agreed to take GAO's recommendations under advisement when modifying its FISMA reporting instructions. Highlights: <http://www.gao.gov/highlights/d07837high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-837>

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

43. *July 27, Insurance Journal* — **RAND Study: Wind insurance scarce on Gulf Coast; challenge for both insurers, government.** Many businesses along the Gulf of Mexico coast have had a difficult time obtaining wind insurance coverage since Hurricanes Katrina, Rita, and Wilma hit in 2005 and have often ended up paying more than twice as much for the insurance as they did previously, according to a recent RAND Corp. study. Gulf Coast businesses are also paying higher wind insurance deductibles while getting lower limits on policy coverage, the study by the nonprofit research organization found. Because they have been increasingly unable to purchase coverage in the regulated, insurance market, business have often turned to state-run residual insurance markets that provide limited insurance to businesses unable to find insurance elsewhere, according to the study conducted for the RAND Gulf States Policy Institute by the RAND Institute for Civil Justice. Researchers found that as wind insurance coverage limits have declined and deductibles have increased, while the use of residual markets has risen, wind risk has shifted in part from insurers to policyholders and taxpayers – including those not living in high-risk areas along the Gulf Coast.

The RAND study, "Commercial Wind Insurance in the Gulf States: Developments Since Hurricane Katrina and Challenges Moving Forward," is available at <http://www.rand.org>.

Source: http://www.insurancejournal.com/news/national/2007/07/27/821_05.htm

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

General Sector

Nothing to report.

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

DHS Daily Open Source Infrastructure Report Contact Information

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

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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov 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.