



# Department of Homeland Security Daily Open Source Infrastructure Report for 24 July 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

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

## Daily Highlights

- The Associated Press reports a blackout affecting an estimated 100,000 people in Queens -- which entered its fifth day Friday, July 21 -- is 10 times worse than the power company Con Edison had previously said. (See item [1](#))
- The Washington Times reports the president of the Border Patrol union told Congress that building fences dramatically reduces crime along high-traffic areas of the U.S. border with Mexico, such as the border area just south of San Diego. (See item [15](#))
- The Associated Press reports three people have pleaded guilty to being part of an ecoterror cell that planted firebombs across the West trying to stop logging, wild horse roundups, sales of sport utility vehicles, and other such activities. (See item [39](#))

### 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 24, Associated Press* — **Con Ed: Blackout's 10 times worse than originally reported.** A blackout affecting an estimated 100,000 people in Queens -- which entered its fifth day Friday -- is 10 times worse than the power company had previously reported, Con Edison said. New York Mayor Michael Bloomberg, speaking on his weekly radio show, said he was "annoyed"

by the new estimate — 25,000 customers without power — because "we might have thrown more resources into the area." Bloomberg later made the "100,000 people" estimate at a news conference. Con Edison said its revised number followed a block-by-block cable inspection in northwest Queens on Thursday night. It said previous estimates came from the number of customers who called to complain. Similarly, Con Edison said Friday that 35,000 customers in Westchester County — not the 25,000 reported earlier — lost power after Tuesday's storm. "They have no way of measuring whether or not there's power to your house" until workers make it to that location, Bloomberg said. "They cannot tell from their computers."

Source: <http://www.nydailynews.com/front/story/436887p-368106c.html>

2. *July 21, Reuters* — **Blackouts from wind, lightning vex utilities.** Power outages that left more than 1.5 million customers without lights this week have fired up criticism that U.S. utilities aren't investing enough to fortify electrical lines against wind, lightning and falling trees. Blackouts in the Midwest and the Mid-Atlantic States left neighborhoods without power just as a heat wave settled across most of the country. Utilities blamed violent storms packing hurricane-force winds that snapped trees and downed power lines. But consumer advocates said the outages point to deeper issues that give the U.S. worse power problems than other developed countries like England, France, and Japan. Some experts say U.S. power companies are cutting costs by spending less money than many other countries to harden infrastructure against Mother Nature. "U.S. power prices are cheaper than in the rest of the world, but we have lower reliability. It is a choice that we've made," said Jay Apt of the Electricity Industry Center at Carnegie Mellon. The U.S. power grid held up well to the strain of record electric use against a nationwide heat wave this summer but saw distribution lines falter in delivering power to individual homes and businesses during the recent storms.

Source: [http://today.reuters.com/news/newsarticle.aspx?type=domesticNews&storyid=2006-07-21T165723Z\\_01\\_N21153431\\_RTRUKOC\\_0\\_US-UTILITIES-WEATHER-BLACKOUTS.xml&src=rss&rpc=22](http://today.reuters.com/news/newsarticle.aspx?type=domesticNews&storyid=2006-07-21T165723Z_01_N21153431_RTRUKOC_0_US-UTILITIES-WEATHER-BLACKOUTS.xml&src=rss&rpc=22)

3. *July 20, Federal Energy Regulatory Commission* — **FERC certifies North American Electric Reliability Council as the nation's ERO.** The Federal Energy Regulatory Commission (FERC) certified the North American Electric Reliability Council (NERC) as the nation's Electric Reliability Organization (ERO), pursuant to the Energy Policy Act of 2005. As the ERO, NERC will be responsible for developing and enforcing mandatory electric reliability standards under the commission's oversight. The standards will apply to all users, owners and operators of the bulk-power system. The commission also granted a petition from the governors of Arizona, California, Colorado, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming to establish a regional advisory body, as provided for under the Energy Policy Act. Both the ERO and Regional Entities will be reviewed periodically to assure the statutory qualifying criteria are maintained on an ongoing basis. All proposed reliability standards must be submitted by the ERO to the commission for its approval. The ERO and Regional Entities must monitor compliance with the reliability standards. They may direct violators to comply with the standards, and impose penalties for violations, subject to review by, and appeal to, FERC. While the ERO is responsible for compliance and enforcement under commission oversight, the statute provides that FERC can investigate compliance and impose penalties independently of the ERO.

Source: <http://www.ferc.gov/press-room/press-releases/2006/2006-3/07-20-06-E-5.asp>

4. *July 20, Reuters* — **Midwest storm cuts power, hits oil infrastructure.** About half a million power customers in Illinois and Missouri remained without electricity on Thursday, July 20, after a storm packing hurricane-force winds slammed the region, shutting one refinery and briefly disrupting oil pipeline operations. Winds of up to 80 miles per hour snapped utility poles and downed powerlines across southwestern Illinois on Wednesday night, knocking out service to around 550,000 customers of Ameren Corp. About 450,000 customers remained without power by midday Thursday. Exelon Corp. said about 21,000 customers in the Chicago area were also without power on Thursday following the storm. ConocoPhillips was forced to shut its 306,000-barrel per day (bpd) Wood River refinery in Roxana, IL, after power to the plant was cut. Trading sources said the refinery was expected to be back on line in three to five days assuming no damage occurred during the shutdown. The power outage forced Kinder Morgan on Wednesday night to shut its 150,000 bpd Platte pipeline, which ships crude from Canada to the U.S. Midwest. Throughput on the pipeline was restarted early Thursday morning. The 700,000 bpd Explorer pipeline was also offline for four hours on Wednesday night due to the power failure.

Source: [http://today.reuters.com/investing/financeArticle.aspx?type=bondsNews&storyID=2006-07-20T192632Z\\_01\\_N20211969\\_RTRIDST\\_0\\_ENERGY-US-STORM.XML](http://today.reuters.com/investing/financeArticle.aspx?type=bondsNews&storyID=2006-07-20T192632Z_01_N20211969_RTRIDST_0_ENERGY-US-STORM.XML)

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

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

Nothing to report.

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

## **Defense Industrial Base Sector**

5. *August 01, National Defense* — **Combat drone project exposes pitfalls of joint-service programs.** When the Pentagon quashed a multibillion-dollar Air Force-Navy combat drone program earlier this year, experts contended this was proof that joint service projects are doomed from the get-go. The complexity of making multi-service aircraft is most evident in systems that are intended for both Air Force and Navy operations. The F-35 joint strike fighter has three variants, but 80 percent of the components are common to all three. Nevertheless, there are stringent specifications that are unique to the Air Force, Navy and Marine Corps. Navy warplanes are particularly demanding because they operate from aircraft carrier decks. They employ different fuels, for example, and must comply with a host of safety regulations that would not apply to aircraft launched from land bases. Navy aircraft have heavier landing gear and the added weight diminishes their range. They are built with special materials and components that can survive in a highly corrosive environment. Even the aerial refueling equipment and the electronic defensive gear are different in Navy and Air Force jets. The shipboard-unique features generally make Navy jets more expensive.

Source: <http://www.nationaldefensemagazine.org/issues/2006/august/CombatDroneProject.htm>

6. *August 01, National Defense* — **Disjointed defense simulation programs prompt reorganization.** The increasing demand for virtual training and war gaming has prompted the

Department of Defense to reorganize how it manages modeling and simulation. Ongoing efforts to integrate disparate modeling and simulation work reflect growing pressures on the armed services to collaborate more closely in weapon systems procurement, research and development, officials said. “We need to do things better and we need to make a collaborative effort across the community,” said Fred Hartman, deputy director of readiness and training policy and programs in the office of the deputy under secretary of defense for personnel and readiness. The Pentagon’s modeling and simulation office was directed seven years ago to show the benefits of “cross–service and cross–community” cooperation, said Hartman. To attain “common and cross–cutting” tools, data and services, the office is transitioning to a modeling and simulation coordination office that will support six communities: training, analysis, acquisitions, testing, planning and experimentation.

Source: <http://www.nationaldefensemagazine.org/issues/2006/august/DisjointedDefenseim.htm>

7. *July 20, Washington Technology* — **DoD report advocates open–source approach for software acquisition.** A recently released Department of Defense (DoD) report on technology development methodologies advocates more use of open–source software and suggests ways it can be incorporated into the procurement cycle. Reuse can save money by promoting reuse of software across the different defense agencies, the report contends. The Office of the Deputy Undersecretary of Defense for Advanced Systems and Concepts commissioned the Open Technology Development (OTD) road map, which was published in April but only recently released publicly. The concept of OTD is based on sharing software code developed by the DoD and its contractors, as well as by the worldwide open–source community. OTD road map: <http://www.acq.osd.mil/actd/articles/OTDRoadmapFinal.pdf>  
Source: [http://www.washingtontechnology.com/news/1\\_1/defense/28963–1.html](http://www.washingtontechnology.com/news/1_1/defense/28963–1.html)

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

## **Banking and Finance Sector**

8. *July 20, Websense Security Labs* — **Phishing Alert: Macquarie Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of Macquarie Bank, based in Australia. Users are given a link to a fraudulent Website, where they are prompted to enter their personal and financial details.  
Source: <http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=555>
9. *July 19, Express–News (TX)* — **Scam claims \$300 card could save your life.** A new phone scam claims that San Antonio, TX, residents must buy a \$300 card to guarantee them fire and ambulance service in an emergency. It comes with the added — and bogus — promise that city emergency workers will have access to the cardholder's medical history, according to the Texas attorney general. San Antonio resident Cynthia McPherson nearly fell for it. The scammer's phone call came last week. A male caller who said he was from EMT Alert Inc. said San Antonio would soon require her to buy a \$300 card so first responders would know her family's special medical needs. He offered to complete the purchase over the phone if she would give him her bank account number. Texas Attorney General Greg Abbott issued a statewide alert Tuesday, July 18, warning consumers about the scam. EMT Alert Customer Service Manager Katy Miller said she is investigating the complaint because the Phoenix–area company's product is not mandatory in any Texas city. So far, McPherson is the first Texan to complain to

local officials about the company, said the attorney general's spokesperson.  
Source: <http://www.mysanantonio.com/business/stories/MYSA072006.6E.BIZemt.scam.a3f2af.html>

**10. July 18, Baltimore Sun — Laundering laws, terror policy hurt check-cashers.** Some national and regional banks are dropping as customers check-cashing operations and other money-service businesses over concerns the firms aren't following federal guidelines meant to thwart money laundering and terrorist financing. Without banking services, a handful of money services businesses have closed in Maryland, according to the state Department of Labor, Licensing, and Regulation. Those businesses often operate in low-income neighborhoods where residents rely on them to cash paychecks and transfer money to families in other countries. Regulators fear those residents might be forced to turn to loan sharks and other illegal means for their banking needs, should more financial institutions follow suit. Bank of America Corp., Provident Bankshares Corp., and SunTrust Banks Inc. are among banks in the Baltimore region that have severed ties with money-service businesses. Check-cashers typically depend on banks to clear checks and provide cash by allowing them to draw against checks that have been deposited but not yet cleared. An estimated 12 million people are classified as "unbanked" in the U.S. Without access to traditional banking such as checking accounts, many use money-service businesses to cash checks or obtain money orders to pay bills.

Source: <http://www.baltimoresun.com/business/investing/bal-bz.checkcash18jul18.0.7469194.story?track=rss>

[[Return to top](#)]

## **Transportation and Border Security Sector**

**11. July 23, Associated Press — Boston tunnel reopens to bus traffic.** A major highway tunnel that carries traffic under Boston Harbor to the airport reopened to buses Friday morning, July 21, a day after the governor ordered it shut down to fix two slipping bolts in a heavy ceiling panel. The tunnels throughout Boston's Big Dig highway system have been heavily scrutinized since a motorist was killed last week by 12 tons of falling concrete ceiling panels. Inspectors discovered more than 1,100 suspect bolts in the ceilings of that tunnel and a tunnel ramp. Governor Mitt Romney ordered the nearby Ted Williams Tunnel's eastbound lanes closed on Thursday, July 20, after state engineers discovered two bolts on a single ceiling panel there appeared to have slipped a half-inch and one inch. Engineers worked through the night to reinforce the bolt systems and the tunnel reopened about 7 a.m. Friday. The Ted Williams Tunnel's ceiling panels are suspended using the same threaded, epoxy bolts as the panels that collapsed, but the Ted Williams Tunnel panels are lighter and the system that suspends them is considered more substantial.

Source: <http://abcnews.go.com/US/wireStory?id=2220179>

**12. July 23, Houston Chronicle — Guard, patrol applaud collaborative border plan.** Inside the U.S. Border Patrol's communications center in Laredo, a Texas Army National Guard soldier sat at a computer Thursday, July 19, and moved his mouse to aim a surveillance camera at the Rio Grande. As he did so, one of dozens of video monitors on the wall before him showed a changing panorama of the river and its rugged banks. The guardsman was being trained to look

for signs of intruders on a 45-mile stretch of border that is watched day and night. Guard and patrol officials said the month-old deployment of troops to the border is working as planned, enabling at least three dozen patrol agents to return to law enforcement duties. More than 100 soldiers have arrived and by the end of August there could be 300, said Lt. Col. Rick Noriega of Houston, commander of guard troops in the patrol's Laredo sector. "We've been able to reach one of our objectives ... to return Border Patrol agents to the border to do the work that agents should be doing as opposed to clerical or camera operations-type surveillance duties," said Patrol Acting Sector Chief Reynaldo Garza.

Source: <http://www.chron.com/disp/story.mpl/metropolitan/4062104.htm>

- 13. July 23, FOX News — Cruise ship that listed on voyage picks up new passengers.** A cruise ship that unexpectedly listed to one side during a trip through calm Atlantic waters picked up a new load of passengers en route to the Caribbean on Saturday, July 22, for its first voyage since the mishap. Investigators on Saturday still were not finished investigating why the Crown Princess suddenly listed 15 degrees Tuesday, July 18, while traveling about 11.5 miles off Port Canaveral. The unexpected lurch threw passengers and unfastened objects against the deck and walls before the ship leveled itself in about 40 seconds, by passenger estimates. Inspectors, however, found that the ship was mechanically safe and cleared it to return to service, according to Coast Guard spokesperson Dan Bender. After some cancellations, the ship is sailing at about 15 percent below its capacity of 3,000 passengers, said Princess Cruise lines spokesperson Julie Benson.

Source: <http://www.foxnews.com/story/0.2933.205132.00.html>

- 14. July 21, Inside Bay Area (CA) — Plan to dramatically expand Bay ferry service.** As the San Francisco Bay Area braces for one million more residents by 2020, transportation officials are hoping a portion of them will commute across the Bay by ferry. Under a regional transit plan in its early stages, the ports of South San Francisco, Redwood City, Hercules, Richmond, Berkeley, Alameda, Treasure Island, and Antioch/Martinez all could become commuter hubs for ferry service to San Francisco. At a meeting of the San Francisco Bay Conservation and Development Commission on Thursday, July 20, officials approved a \$20,000 contract to consult with the Metropolitan Transportation Commission on the water transit project, in the works since 1999. The \$500 million project, which would also involve erecting concentrated housing near many of the new transit hubs, is further along in some cities than others. South San Francisco's Oyster Point Marina is expected to begin ferry service to Oakland in 2008, and Berkeley's service to San Francisco could start as early as 2009, according to Steve Castleberry, head of the San Francisco Bay Area Water Transit Authority. About 10,000 Bay Area residents use existing ferry service for their daily commute at present, according to Castleberry.

Source: [http://www.insidebayarea.com/oaklandtribune/ci\\_4078339](http://www.insidebayarea.com/oaklandtribune/ci_4078339)

- 15. July 21, Washington Times — Border fence cited as deterrent to crime.** Building fences along high-traffic areas of the U.S. border with Mexico dramatically reduces crime, the president of the Border Patrol union told Congress on Thursday, July 20. "Drug smuggling was rampant" in the border area just south of San Diego, said T.J. Bonner, national president of the National Border Patrol Council, before a fence was constructed. Bonner said that after the fence was built, with surplus military steel landing mats, drug seizures tapered off and the crime rate fell sharply. Most Congress members at the joint hearing yesterday seemed to agree on the need for fencing. The hearing was part of a series of House hearings into the Senate immigration

reform bill. Though the fences curb crime, Bonner said they will do little to stop illegal entry if supplementary efforts are not undertaken. The only way to control the borders, he said, is to increase the number of Border Patrol agents and remove the magnet of potential U.S. employment.

Source: <http://www.washtimes.com/national/20060720-105104-9512r.htm>

16. *July 21, Washington Post* — **Suspicious packages cause alarm at Union Station.** Police evacuated Washington, DC's Union Station Thursday night, July 20, after bomb-sniffing dogs reacted to three suspicious packages, triggering train delays as far north as Boston, authorities said. After more than two hours, the packages were found to be harmless, containing food and clothing. The discovery shortly before 8 p.m. EDT of a suitcase, a garbage bag, and a box in the station's lost and found area disrupted the schedules of about 10 Amtrak trains. Some people on local trains were forced to get off at New Carrollton and Alexandria stations, and restaurants and bars in the station were closed as the building was evacuated. Employees and anxious travelers waited in the wilting heat outside the station as police, firefighters, bomb technicians and members of the FBI Joint Terrorism Task Force converged to examine the packages and secure the area.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/21/AR2006072100002.html>

17. *July 21, Associated Press* — **Texas airport unveils podcasts.** Dallas-Fort Worth International Airport (DFW) officials on Thursday, July 20, announced a series of free podcasts in English and Spanish to provide travelers with information about parking, restaurants and shopping. The podcasts, available in audio and video formats, can be downloaded at the airport's Website or via Apple's iTunes Music Store. According to DFW Airport Chief Operating Officer Kevin Cox, the airport is the first in the world to offer podcasts. The initial release of four podcasts are between one and three minutes long and include an overview of restaurants at the airport's international terminal and parking directions. Another upcoming podcast will explain how to use the airport's train system. One thing the podcasts won't provide is information on flights or connecting gates, he said.

Source: [http://www.usatoday.com/travel/flights/2006-07-21-dfw-podcasts\\_x.htm](http://www.usatoday.com/travel/flights/2006-07-21-dfw-podcasts_x.htm)

18. *July 21, Associated Press* — **American seeks second U.S.-China route.** American Airlines said Thursday, July 20, it is seeking permission for a second route to China and hopes to offer daily non-stop service between Dallas and Beijing beginning in March 2007. American, the largest U.S. carrier, said it had filed an application for the route with the Department of Transportation. The timing would let American benefit from the 2008 Olympics in Beijing and from increased ties between China and corporations based in the Dallas area. Airlines, like other U.S. businesses, are eager to serve China's huge population and rapidly growing economy. The bid for new China flights pits Fort Worth-based American against Houston-based Continental Airlines, which is seeking approval to fly from Newark, NJ, to Shanghai. The Texas airlines already operate flights to China — American serves the Chicago-Shanghai route, while Continental flies from Newark to Beijing. But both are chasing two early entrants in the market — United Airlines and Northwest Airlines.

Source: [http://www.usatoday.com/travel/flights/2006-07-21-american\\_china\\_x.htm](http://www.usatoday.com/travel/flights/2006-07-21-american_china_x.htm)

19.

*July 20, Department of Transportation* — **BP Exploration directed to complete testing on North Slope pipelines.** The Pipeline and Hazardous Materials Safety Administration (PHMSA) on Thursday, July 20, directed BP Exploration (Alaska) Inc. to take additional measures to ensure safety on its Prudhoe Bay pipelines as a result of a pipeline failure in March 2006. The agency’s latest directive requires BP to submit a comprehensive engineering plan to safely and quickly drain 17,000 barrels of oil contained within the idled Western Operations Area pipeline, and requires completion of engineering plans to assure sediment within the pipelines is stored safely in tanks to avoid contamination and maintain the safety of the Trans Alaska Pipeline system. PHMSA Administrator Tom Barrett and acting Chief Safety Officer Stacey Gerard visited Alaska earlier this month to review North Slope pipeline operations, meet with federal and state officials, and ensure completion of the corrective actions required by PHMSA’s original order. “These additional corrective actions are needed to assure the safety of the pipeline operations,” said PHMSA Administrator Barrett. “BP’s operations must reflect suitable and stringent operational controls.” PHMSA is coordinating its actions with the federal–state Joint Pipeline Office and with numerous federal and state agencies that oversee the safety on the North Slope of Alaska.

Source: <http://www.dot.gov/affairs/phmsa0506.htm>

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

## **Postal and Shipping Sector**

20. *July 20, East Texas Review* — **New scam, counterfeit U.S. Postal money order.** According to Texas Attorney General Gregg Abbott, “recently, in a troubling new twist, Texas financial institutions and consumers have been reporting the existence of high quality counterfeit U.S. Postal money orders that are being used to fool consumers into cashing them and wiring part of the money abroad. Finding that consumers have caught on to the counterfeit check scam, scammers are now using phony U.S. Postal money orders instead of cashier’s checks. Cashier’s checks and postal money orders are generally considered much safer than personal checks, since they are issued by financial institutions that have already verified the existence of sufficient funds. These counterfeits are so good sometimes that even bank tellers have been fooled.”

Source: <http://www.easttexasreview.com/story.htm?StoryID=3712>

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

## **Agriculture Sector**

21. *July 22, Agence France–Presse* — **Swine fever epidemic hits eastern Croatia.** The outbreak of classical swine fever (CSW) in eastern Croatia, the first in the Balkans country since 2003, has turned into an epidemic, a minister said. The presence of swine fever was confirmed earlier this month at three breeding sites in the region of the eastern town of Vukovar. So far a total of 264 pigs which were either infected or suspected to have caught the disease were slaughtered to prevent its spread. In 21 of 550 family farms which have been inspected so far the presence of the swine fever virus has been confirmed.

CSW information: [http://www.oie.int/eng/maladies/fiches/a\\_A130.htm](http://www.oie.int/eng/maladies/fiches/a_A130.htm)

Source: [http://news.yahoo.com/s/afp/20060722/hl\\_afp/croatiahealthfarm\\_060722201747](http://news.yahoo.com/s/afp/20060722/hl_afp/croatiahealthfarm_060722201747)

**22. July 20, Reuters — Anthrax hits livestock in Western Canada, U.S.** At least 234 cattle and other livestock have died in the Canadian Prairies, following the country's second anthrax outbreak this summer, officials said on Thursday, July 20. The latest outbreak has killed 24 cattle and one horse from four different herds in southeastern Manitoba, the provincial government said. Four farms have been quarantined and the affected animals did not enter the food chain, the Canadian Food Inspection Agency said. Saskatchewan, Canada, which borders Manitoba to the west, first reported its anthrax outbreak in late June. The CFIA said on Thursday that 209 cattle and other livestock had died, up from the 175 reported dead the day before. Farms were placed under 21-day quarantines and on Thursday, the federal food safety agency stated that 48 farms remained under quarantine as positive premises. At least 8,500 animals have been vaccinated and both outbreaks were considered under control. In Minnesota, which borders Manitoba to the south, 68 cattle and other livestock have died from anthrax since mid-June, the Minnesota Board of Animal Health said.

Source: [http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006-07-20T205144Z\\_01\\_N20289090\\_RTRUKOC\\_0\\_US-FOOD-CANADA-ANTHRAX.xml&archived=False](http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006-07-20T205144Z_01_N20289090_RTRUKOC_0_US-FOOD-CANADA-ANTHRAX.xml&archived=False)

**23. July 20, U.S. Department of Agriculture — Funds to stop the spread of emerald ash borer announced.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Thursday, July 20, announced the availability of an additional \$7.6 million in emergency funding for emerald ash borer (EAB) eradication efforts in Illinois and Wisconsin. This brings total funding for EAB eradication efforts across the U.S. in 2006 to \$25 million. The funds will be used to conduct an intensive survey program and quarantine affected areas in Illinois to prevent additional EAB spread. The Animal and Plant Health Inspection Service (APHIS) and Illinois Department of Agriculture officials have already begun survey activities to determine the extent of the infestations discovered in Wilmette and the nine counties surrounding Kane County, which include areas in Wisconsin. APHIS is preparing an interim rule for publication in the Federal Register to implement a quarantine to prevent the movement of host materials (nursery stock, firewood, etc) out of the area. The quarantine may be expanded if additional areas are found to be infested. In addition to the survey, regulatory and control activities, these funds will also support an aggressive outreach and education campaign to enlist the support and cooperation of homeowners and businesses.

EAB information: <http://www.emeraldashborer.info/>

Source: <http://www.usda.gov/wps/portal/!ut/p/.s.7.0.A/7.0.1OB?contentonly=true&contentid=2006/07/0260.xml>

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

## **Food Sector**

**24. July 21, Agence France-Presse — Japan to resume U.S. beef imports.** Japan will give the final green light the week of July 24 to resume U.S. beef imports banned over mad cow disease, ending a long rift with its closest ally, a report has said. Japan announced in June that it had agreed to the conditions for resuming US beef imports but said it would first inspect 35 meatpacking factories in the U.S. The inspectors have approved conditions in the factories, Jiji

Press said. It said the government would make a final decision next week, with beef shipments to resume by the end of the month. Japan first banned US beef in December 2003 after a cow infected with bovine spongiform encephalopathy (BSE) was discovered in the state of Washington. It lifted the ban in December 2005 but slapped the embargo back on just a month later when a U.S. shipment violated safety guidelines that required the removal of high risk material such as the animals' spines.

Source: [http://news.yahoo.com/s/afp/20060721/pl\\_afp/healthjapanustra\\_demadcow\\_060721120045;\\_ylt=Aq1LpA\\_bo.pydASit5DbSuyJOrgF;\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060721/pl_afp/healthjapanustra_demadcow_060721120045;_ylt=Aq1LpA_bo.pydASit5DbSuyJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)

25. *July 20, Associated Press* — **Illnesses traced to uncooked chicken entrees.** Minnesota food safety officials issued a warning Thursday, July 20, about some frozen stuffed chicken entrees that contain uncooked chicken. Investigators from the state health and agriculture departments said 29 people in Minnesota have become ill after eating frozen chicken entrees that weren't cooked long enough to kill salmonella bacteria. They are usually pre-browned, but contain raw chicken. Most of the cases were traced to products manufactured by Aspen Foods in Chicago, IL, and Serenade Foods of Milford, IN, and sold under a variety of brand names, including store brand names, state officials said. The U.S. Department of Agriculture issued a limited recall in March 2006 after the salmonella outbreak was identified. However, epidemiologists have found that new cases of illness continue to occur.

Source: <http://www.duluthsuperior.com/mld/duluthsuperior/15085396.htm>

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

## Water Sector

26. *July 21, Honolulu Star-Bulletin* — **Partially treated sewage spills offshore.** Nearly 600,000 gallons of partially treated sewage was discharged Wednesday, July 19, from a deep-ocean pipe for the Honouliuli Wastewater Treatment Plant, according to city officials. The Barbers Point "outfall" pipe is more than two miles offshore, at a depth of 200 feet, "so the bypass is expected to have negligible effects on the environment." Although the spill happened on Wednesday afternoon, city officials did not issue a news release Thursday evening. When spills occur on land or in nearshore waters, city officials "have to do a press release right away, and signage and sampling is right away, like clockwork," said Watson Okubo, who is in charge of water quality testing for the state. But Okubo was not sure of the protocol when the incident is at a deep-ocean outfall.

Source: <http://starbulletin.com/2006/07/21/news/story09.html>

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

## Public Health Sector

27. *July 22, Xinhua* — **China reports new bird flu outbreak.** A new bird flu outbreak has been identified in northwestern Xinjiang Uygur Autonomous Region, according to the Ministry of Agriculture. The outbreak occurred on July 14 in a community in Xinjiang's Aksu city, and the H5N1 virus was found in the samples of the dead poultry by the national bird flu laboratory,

said the ministry. The H5N1 strain of avian flu had killed 3,045 chickens, and another 356,976 head had been culled in an emergency response.

Source: [http://www.chinadaily.com.cn/china/2006-07/22/content\\_647019.htm](http://www.chinadaily.com.cn/china/2006-07/22/content_647019.htm)

28. *July 21, Reuters* — **Share of U.S. doctors using digital records up a bit.** Nearly a quarter of U.S. physicians used some form of electronic patient record in 2005, as officials try to meet a presidential goal of having digital health data for every American by 2014. "Although these estimates show that progress has been made toward the goal of universal electronic health records, there is still a long way to go," U.S. Centers for Disease Control and Prevention (CDC) statisticians said. About 24 percent of doctors in 2005 said they used electronic health records, either entirely or in combination with paper, compared with 21 percent in 2004. The CDC survey of 1,281 doctors found gaps between large medical practices and smaller doctor groups. About 46 percent of doctors in groups with 11 or more use some form of electronic records compared with 16 percent in solo practices.

Source: [http://today.reuters.com/stocks/QuoteCompanyNewsArticle.aspx?view=CN&storyID=2006-07-21T225659Z\\_01\\_N21314440\\_RTRIDST\\_0\\_HEALTH-TECHNOLOGY.XML&rpc=66](http://today.reuters.com/stocks/QuoteCompanyNewsArticle.aspx?view=CN&storyID=2006-07-21T225659Z_01_N21314440_RTRIDST_0_HEALTH-TECHNOLOGY.XML&rpc=66)

[[Return to top](#)]

## Government Sector

Nothing to report.

[[Return to top](#)]

## Emergency Services Sector

29. *July 21, Providence Journal (RI)* — **Most in charge of the disaster response are volunteers with little training or funds.** In a disaster, local emergency management directors must make key decisions, from ordering evacuations to opening shelters, getting food and water to residents and clearing debris. They must also recruit volunteers and get them trained for emergencies. Federal and state agencies rely heavily on guidance from local officials. But only two Rhode Island communities — Providence and Pawtucket — have full-time emergency directors. The rest are volunteers or part-timers, many with little or no funding and minimal experience in emergency planning. Many part-time directors say they are torn between their regular jobs and emergency management. It's not surprising that smaller communities have minimal budgets. But even cities such as Cranston, Newport and Warwick rely on their fire chiefs to double as emergency directors, using money from their own budgets. Many of the directors expressed frustration at the increased demands. "It would take several full-time employees just to do the paperwork," said Barrington's part-time Emergency Management Agency director Victor Teixeira. Some are confused about their new responsibilities — and that means local emergency planning is uncoordinated and mixed across the state.

Source: [http://www.projo.com/news/content/projo\\_20060721\\_ema21.164b1\\_da.html](http://www.projo.com/news/content/projo_20060721_ema21.164b1_da.html)

30. *July 21, Advocate (LA)* — **Evacuation an issue for Louisiana trailer park.** Almost two months after an emergency drill at the Federal Emergency Management Agency's (FEMA)

Renaissance Village, questions remain over how to evacuate the parish's largest trailer park for hurricane evacuees. Yvonne Murphy, chief of operations for East Baton Rouge, LA, Parish's Office of Homeland Security and Emergency Preparedness, said her agency still isn't sure how to communicate with FEMA trailer residents or coordinate an evacuation during a hurricane or other disaster. East Baton Rouge Parish has 1,884 occupied FEMA trailers, according to FEMA. Murphy said that during a May exercise to test readiness for the current hurricane season, efforts to contact and move people out of the Baker-area trailer park failed. Local officials at the time said the drill was aborted after they couldn't get the authorization they believed was needed to enter the site and evacuate people playing the role of Renaissance Village residents.

Source: <http://www.2theadvocate.com/news/3395391.html>

**31. *July 20, Washington Technology* — FEMA crafts credentialing system for first responders.**

FEMA crafts credentialing system for first responders Documentation for millions of police, firefighters, medical workers and other emergency personnel nationwide is being aggregated into a National Emergency Responder Credentialing System that the Department of Homeland Security (DHS) expects to make operational next year. At a future date, the new credentialing system may include a national identification card for emergency responders and a record-keeping system, according to a DHS fact sheet published on project. The little-publicized credentialing system is intended to assist in identifying which responders should be allowed to enter an incident scene immediately following a disaster or terrorist attack. It is designed to help prohibit unauthorized entry of volunteers who may not be qualified to assist.

DHS Fact Sheet: [http://www.fema.gov/pdf/emergency/nims/credent\\_faq.pdf](http://www.fema.gov/pdf/emergency/nims/credent_faq.pdf)

Source: [http://www.washingtontechnology.com/news/1\\_1/homeland/28965-1.html](http://www.washingtontechnology.com/news/1_1/homeland/28965-1.html)

**32. *July 20, Government Accountability Office* — GAO-06-826: Disaster Preparedness: Limitations in Federal Evacuation Assistance for Health Facilities Should Be Addressed (Report).**

Hurricane Katrina demonstrated difficulties involved in evacuating communities and raised questions about how hospitals and nursing homes plan for evacuations and how the federal government assists. Due to broad-based congressional interest, the Government Accountability Office (GAO) assessed the evacuation of hospital patients and nursing home residents. Under the Comptroller General's authority to conduct evaluations on his own initiative, GAO examined (1) the challenges hospital and nursing home administrators faced, (2) the extent to which limitations exist in the design of the National Disaster Medical System to assist with patient evacuations, and (3) the federal requirements for hospital and nursing home disaster and evacuation planning. GAO reviewed documents and interviewed federal officials, and interviewed hospital and nursing home administrators and state and local officials in areas affected by Hurricane Katrina in Mississippi and Hurricane Charley in Florida. GAO recommends that the Department of Homeland Security (DHS) clearly delineate (1) how the federal government will assist state and local governments with the transportation of patients and residents out of hospitals and nursing homes, and (2) how to address the needs of nursing home residents during evacuations.

Highlights: <http://www.gao.gov/highlights/d06826high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-826>

33.

*July 19, Stateline* — **Governors plan attack on avian flu.** If an avian flu pandemic strikes, states will need to cope not just with severe strain on their hospitals but also with a serious impact on stores, schools, power plants and office cubicles, according to a report released Tuesday, July 18. Governors would have a tough time just keeping basic services going. As many as 40 percent of workers might stay home for a period of up to 14 months, and outside help from the federal government or other states would be severely limited, the National Governors Association (NGA) warned in the report. A key consideration for policy-makers will be the depleted workforce that a pandemic would likely cause. The 32-page document released by the NGA's Center for Best Practices is meant to help governors and their staffs prepare for the unique problems posed by pandemics.

NGA Report: <http://www.nga.org/Files/pdf/0607PANDEMICPRIMER.PDF>

Source: <http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=127998>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

**34. *July 21, Newsfactor Magazine* — MySpace banner ad infects million users.** A banner advertisement posted on the MySpace Website may have infected more than one million users with adware, according to security firm iDefense. The advertisement was included in user profiles on MySpace and could have been operating for about one week. The deckoutyourdeck.com advertisement exploited a flaw in the way Microsoft's Internet Explorer (IE) browser handles Windows Metafile image files. Users running unpatched versions of IE would never have realized that the banner ad had silently installed programs that generate pop-up ads on their system.

Source: [http://www.newsfactor.com/story.xhtml?story\\_id=11100AT9AXG3](http://www.newsfactor.com/story.xhtml?story_id=11100AT9AXG3)

**35. *July 21, Networking Pipeline* — Wi-Fi phone market to soar to \$3.7 billion by 2009: Report.** The Wi-Fi phone market will double every year between now and 2009, and reach \$3.7 billion by that year, according to a new report by Infonetics Research. The report found that the worldwide Wi-Fi phone market increased 116 percent from 2004 to 2005 to reach \$125.5 million, driven by enterprises and consumers deploying voice over wireless networks. The report says that voice over wireless networks are being initially used primarily by enterprises rather than consumers, but that ultimately, it will become popular with consumers as well, as part of a complete a VoIP service bundled with broadband connections.

Report: [http://www.infonetics.com/resources/purple.shtml?ms06.wip.2\\_nr.shtml](http://www.infonetics.com/resources/purple.shtml?ms06.wip.2_nr.shtml)

Source: <http://www.networkingpipeline.com/showArticle.jhtml?articleID=190900665>

**36. *July 20, eWeek* — PowerPoint zero-day attack points to corporate espionage.** A second Trojan used in the latest zero-day attack against Microsoft Office contains characteristics that pinpoint corporate espionage as the main motive, according to virus hunters tracking the threat. According to an alert from Symantec, a backdoor called Trojan.Riler.F is installing itself as a layered service provider, or LSP, allowing it access to every piece of data entering and leaving the infected computer. An LSP is a legitimate system driver linked deep into the networking services of Windows. Symantec said the Trojan also opens a back door on the compromised system and connects to the "soswxyz.8800.org" domain. The Trojan then listens and waits for

commands from a remote attacker.

Symantec Alert: [http://www.symantec.com/enterprise/security\\_response/writeup.jsp?docid=2006-071812-3213-99&tabid=1](http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-071812-3213-99&tabid=1)

Source: <http://www.eweek.com/article2/0.1895.1992128.00.asp>

**37. July 20, eWeek — Spyware fades to a dull roar, but targeted attacks loom.** Analysts agree that most enterprises have reached a point where they can effectively block many forms of spyware, but targeted attacks at specific companies and the need to further integrate security technologies are both keeping businesses on their toes. Much as in their battle against unsolicited spam e-mail, enterprises are having success in reducing the impact of spyware programs, but a new breed of targeted attacks combined with a constantly changing array of delivery methods has kept the malicious code on IT administrators' radar. The challenge for enterprises moving forward, analysts say, will be in warding off spyware attacks crafted by organized criminals that are specifically aimed at their companies, or smaller groups of businesses, and pulling together disparate security technologies to help fight so-called blended threats that use spyware along with other malicious programs to help find new ways onto corporate networks.

Source: <http://www.eweek.com/article2/0.1895.1992007.00.asp>

**38. July 20, CNET News — UK Webmaster accused of aiding terrorists.** British police have arrested a UK citizen on charges that he operated Islamic fundamentalist Websites that preached "violent jihad." The arrest of Syed Talha Ahsan on Wednesday, July 19, came at the request of the U.S. government, which released a 14-page indictment accusing him of selling books, videotapes, audio cassettes, and CD-ROMs that glorified "violent jihad in Chechnya, Bosnia, Afghanistan" and funneling money to groups that were deemed illegal by the federal government. The Websites, including azzam.com, azzam.co.uk, qoqaz.net and qoqaz.co.uk, tout the virtues of jihad, primarily against the West and allied nations.

Indictment: <http://www.usdoj.gov/usao/ct/Documents/AHSAN%20Syed%20Talha%20Indictment.pdf>

Source: [http://news.com.com/U.K.+Webmaster+accused+of+aiding+terrorists/2100-1028\\_3-6096818.html?tag=nefd.top](http://news.com.com/U.K.+Webmaster+accused+of+aiding+terrorists/2100-1028_3-6096818.html?tag=nefd.top)

### Internet Alert Dashboard

#### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of active exploitation of a new vulnerability in Microsoft PowerPoint. Successful exploitation could allow a remote attacker to execute arbitrary code with the privileges of the user running PowerPoint.

For more information please review the following vulnerability note:

**VU#936945:** Microsoft PowerPoint contains an unspecified remote code execution vulnerability. <http://www.kb.cert.org/vuls/id/936945>

US-CERT strongly recommends the following until an update, patch, or more information becomes available:

Do not open attachments from unsolicited email messages.

Install anti virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

US-CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04-010 for more information on working with email attachments. <http://www.us-cert.gov/cas/tips/ST04-010.html>

US-CERT will continue to update current activity as more information becomes available.

### **PHISHING SCAMS**

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

### **Current Port Attacks**

<b>Top 10 Target Ports</b>	44139 (----), 1026 (win-rpc), 4672 (eMule), 50497 (----), 445 (microsoft-ds), 38566 (----), 32790 (----), 80 (www), 135 (epmap), 113 (auth)
----------------------------	---

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](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**

Nothing to report.

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

## **General Sector**

**39. July 23, Associated Press — Six ecoterror cell members enter guilty pleas in fires across West.** Three people pleaded guilty on Friday, July 21, to being part of an ecoterror cell that planted firebombs across the West trying to stop logging, wild horse roundups, genetic engineering of plants, sales of sport utility vehicles, and expansion of a ski resort into endangered lynx habitat. Three others pleaded guilty on Thursday, July 20, three are fugitives, and four are scheduled to go on trial on October 31. William C. Rodgers, described as the group's leader, committed suicide in jail in Arizona just before he was to be sent to Oregon to face charges. The 16 attacks, from 1996 to 2001, did \$20 million in damage in Oregon, Washington, California, Wyoming and Colorado. The Earth Liberation Front and the Animal Liberation Front claimed responsibility. The three who pleaded guilty on Friday admitted to trying to intimidate and coerce federal agencies, private businesses and the public through sabotage and mass destruction.

Source: <http://www.nytimes.com/2006/07/23/us/23eco.html>

**40. July 21, Washington Post — Serial slayings put Phoenix residents on edge.** Phoenix is on edge, not just because of the Baseline Killer but also because of another one known as the Serial Shooter. Together, the two have killed at least 11 people in the past year, police said. Investigators said that the Baseline Killer, named for his initial crimes along Baseline Road, launched his crime binge last August. Since then, police said he has killed five women and one man, and committed seven rapes and eight robberies. Descriptions of him vary, leading detectives to theorize he may wear disguises. Operating independently from the Baseline Killer is the Serial Shooter. The shooter has killed five people, three horses, and five dogs since May 2005, investigators said. The shooter, who targets people outside at night, also is thought to have wounded another 16 people and four animals. Police say they do not have enough evidence to be certain that the Serial Shooter, despite the moniker, is one person. It is not unusual for two or more serial killers to operate at the same time in large American cities, said James Alan Fox, a professor of criminal justice at Northeastern University in Boston and the author of five books on serial killers.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/21/AR2006072101352.html>

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

### **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.