Department of Homeland Security Daily Open Source Infrastructure Report for 28 July 2006

Current Nationwide Threat Level is ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Edison Electric Institute's weekly survey of electric demand reports the U.S. has broken the all−time weekly demand record for electricity during the current national heat wave, surpassing by more than one percent last year's record power usage. (See item 1)
- The Associated Press reports TXU Electricity Delivery is hiring off−duty police officers and security personnel to protect copper wire at some of its substations, and replacing stolen copper with a less valuable metal. (See item 2)
- Reuters reports emergency room professionals have told Congress that a lack of staff, space, and equipment continues to hobble the U.S. emergency medical system, and almost no steps have been taken to improve things despite numerous warnings. (See item 29)
- USA TODAY reports the U.S. Marshals Service −− charged with protecting federal judges, prosecutors, jurors and court employees −− says threats against federal judges and other court employees have reached record numbers. (See item 32)

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 27, Clean Edge News* — **U.S. breaks all−time weekly demand record for electricity during national heat wave.** U.S. demand for electricity reached an all−time record last week amid a punishing national heat wave as U.S. utilities delivered 96,314 gigawatt hours (GWh) of electricity for the week ending July 22, surpassing by more than one percent last year's record of 95,259 GWh (set during the week ending July 23, 2005), according to the Edison Electric Institute's weekly survey of electric demand. Individual utilities and regional grid operators saw their own records shatter as well, and from coast to coast, utilities are scrambling to satisfy the demand for power as searing temperatures continue to blanket much of the country, said EEI President Tom Kuhn. Kuhn said that nearly 750 billion kilowatt− hours have been saved during the past 15 years because of industry efficiency programs. Kuhn said utilities are significantly increasing investment in high−voltage power transmission lines as well as local distribution infrastructure. Nationally, utilities will spend about $6 billion this year for transmission infrastructure and about $14 billion to maintain and upgrade local distribution systems, Kuhn said, adding that additional power plants are also under construction to help meet demand.
   Source: http://www.cleanedge.com/story.php?nID=4224

2. *July 26, Associated Press* — **TXU to hire guards, defend copper from theft.** More people are risking their lives to steal copper, prompting TXU Electricity Delivery to hire off−duty police officers and security personnel to protect the wire at some of its substations. TXU Electricity Delivery, which is based in Dallas, TX, said Wednesday, July 26, it also will replace stolen copper with a less valuable metal, install lighting, update security systems at facilities, and partner with local law enforcement to catch metal thieves. TXU lost $633,000 last year to copper theft, not including the cost of the accompanying power outages, said TXU spokesperson Carol Peters. Jim Owen of the Edison Electric Institute, said he has heard from many members worried about increasing metal thefts. "Different companies are handling this in different ways, and some have been more agressive than others," Owen said. Peters said copper theft can also endanger substation workers if important safety equipment is purloined. Peters said the company has occasionally employed security since 1989 when copper thefts were an intermittent problem, but TXU is now seeing an unprecedented rate of theft, she said.
   Source: http://www.contracostatimes.com/mld/cctimes/business/1512965 6.htm

3. *July 26, SecurityFocus* — **SCADA system makers pushed toward security.** Idaho National Laboratory and the New York State Office of Cyber Security and Critical Infrastructure have teamed up with utilities and makers of distributed control system software to offer advice on how to make system security a major part of the critical infrastructure. Later this week, the group will release the latest draft of a set of guidelines for utilities and manufacturers that offers specific requirements for suppliers of supervisory control and data acquisition (SCADA) systems. The guidelines aim to elevate system security to an explicit part of negotiations between customer and supplier with the goal of making the next generation of critical infrastructure systems more secure than today's software and hardware. "We think we can identify the common weaknesses in regards to security and also identify places were the technology's security can be tightened up," said Michael Assante of Idaho National Laboratory. The security issues of real−time control systems, of which the best known are SCADA systems, has become a focus of both private industry and the government as worries mount that such systems could be used as the vector for a criminal or terrorist attack.
   Source: http://www.securityfocus.com/print/news/11402

4. *July 26, Physics Web* — **Superconducting wire breaks record.** A U.S. firm claims to have sent commercial levels of electric current down long lengths of "second generation" high−temperature superconducting wire for the first time. American Superconductor says that its breakthrough achievement could speed up the acceptance of high−temperature superconductor technology in the market place. The firm's second−generation wire −− made from yttrium, barium copper and oxygen (YBCO) −− is cheaper to manufacture and retains its superconducting abilities better under magnetic fields than "first−generation" wire. The firms says its wires can carry a current of up to 140 Amperes when cooled with liquid nitrogen −− about 150 times as much as a standard copper wire of the same dimension. "Just one of these wires would be able to carry enough power to serve the needs of approximately 1000 homes," says Alex Malozemoff of American Superconductor. The new wires could be used for power transmission and distribution cables, propulsion motors, power regulators, and fault current limiters as well as in prototype power cables, maglev trains, and MRI.
Source: http://physicsweb.org/articles/news/10/7/11/1

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *July 27, KUTV (UT)* — **Hydrochloric acid spill in Utah prompts business evacuation, freeway closure.** Thousands of gallons of spilled hydrochloric acid in Salt Lake City Wednesday, July 26, kept Hazmat crews on edge overnight when it then threatened to eat away at a nearby tank of sulfuric acid. The spill happened on the property of LA Gas in an industrial area. Strong winds are believed to have blown over an elevated tank of hydrochloric acid, spilling at least 13,000 gallons of the corrosive liquid. Businesses within a two−block radius were evacuated. The spill also forced the freeways in the area to be shut down.
Source: http://kutv.com/local/local_story_207205719.html

[Return to top]

Defense Industrial Base Sector

6. *August 01, National Defense* — **Small steps taken in long quest for net−centric military.** The vision has been out there for a long time: a network−centric world where information among military programs or branches can be accessed by commanders or decision makers in a timely manner. Every year, chief information officers, intelligence personnel, generals and academics make their way to net−centric conferences in four−star hotels. While those who attend such conferences say they fully embrace the idea of a net−centric world, there are many in the military who are resistant to change. Many claim that the roadblocks preventing interoperable communications are mostly cultural, rather than technical. There needs to be an investment in the “material network” and the “social network,” said John A. Garstka, assistant director of concepts and operations at the Department of Defense's office of force transformation. Chief information officers, when investing in a new program, don’t always have a firm grip on the “people component,” he added. “The human element is the great unknown here,” Garstka said. Bureaucratic knife fights −− between those who want to maintain control of the information and those who think they should have access to it −− may be the

result if cultural issues are not addressed, he said.
Source: http://www.nationaldefensemagazine.org/issues/2006/August/Sm allstepstaken.htm

7. *July 26, U.S. Air Force* — **General Moseley: New long−range bomber on horizon for 2018.** A new bomber scheduled for operation as early as 2018 will enhance America's long−range strike capabilities, according to Air Force Chief of Staff General T. Michael Moseley in a recent Armed Services Committee speech. In a step to develop future long−range strike capabilities, Air Combat Command is conducting a study that is looking at aircraft platforms and weapon improvements. Air Force leaders will use the study to decide the best pathway for providing long−range strike capabilities for the future Air Force. This process normally takes about two years, but the 2018 target requires accelerated efforts. The new bomber is necessary to recapitalize the Air Force's fleet of B−52 Stratofortress and B−1 Lancer "legacy bombers," and to counter advanced anti−access systems of America's enemies, said Lt. Col. Kevin Shorb, chief of Air Combat Command's Next Generation Long Range Strike Division. In the speech, Moseley said the current bomber fleet is adequate to meet America's needs today, despite its age −− but that's likely to change in the future without a new platform. Colonel Shorb said the platform should meet the needs of a leaner Air Force by reducing aircraft, sorties and fuel needed to put bombs on target.
Source: http://www.af.mil/news/story.asp?id=123024081

8. *July 26, U.S. Department of Defense* — **Unmanned Aircraft give military added capability.** The instant feedback of information supplied by unmanned aerial vehicles (UAVs) is bringing immediate "value added" to U.S. military operations, the Joint Staff's director for strategic plans and policy explained Tuesday, July 25. "UAVs have become such an important tool for our decision makers −− operational battlefield decision makers and strategic decision makers," Air Force Lt. Gen. Victor E. "Gene" Renuart Jr. said in a Pentagon Channel interview. The U.S. military has used UAVs for many years, but their use has rapidly increased and evolved over the past few years, Renuart said. Numerous UAV prototypes have been developed over the past two decades, including hand−launched, slingshot−launched, truck−launched, ship−launched and traditional runway−launched versions. Maritime security is one area in which UAVs are becoming increasingly necessary.
Source: http://www.defenselink.mil/news/Jul2006/20060726_5762.html

[Return to top]

Banking and Finance Sector

9. *July 27, Bankok Post (Thailand)* — **Credit card skimming rife at top tourist spots, police warn.** Police are advising credit card users to be more cautious when using them at major tourist spots following the arrest of a criminal who stole electronic data through tapping of phone lines used to confirm payment. The information was then sent to Malaysia and used to make fake cards. Pattaya, Hua Hin, Koh Samui, Chiang Mai, and Mae Hong Son, Thailand, top the list of popular tourist destinations where credit card fraud has recently been reported. The police warning follows the arrest of Thosapol Chaowanawut, 42, in Bangkok on Tuesday, July 25. He was found to be using equipment to intercept the modulated signals containing the sensitive data which is sent from a terminal to a bank for verification. The information was recorded on MP3 players. It was estimated he stole data from more than 10,000 credit card

users.
Source: http://www.bangkokpost.com/News/27Jul2006_news11.php

10. *July 26, Computerworld* — **Missing laptop with data on 540,000 New York state workers found.** A laptop computer containing personal information on more than half a million New York state workers has been found after it disappeared May 9 from the offices of a third−party data management company. In a statement Wednesday, July 26, CS Stars said the laptop belonging to the New York Special Funds Conservation Committee "has been found and secured." Al Modugno of CS Stars would not comment on whether it had been lost or stolen. Modugno said the FBI told CS Stars that the agency is reasonably certain that there was no improper use of any of the data stored on the laptop. The laptop contains the names, addresses, and Social Security numbers of about 540,000 state employees.
Source: http://www.computerworld.com/action/article.do?command=print ArticleBasic&articleId=9002031

11. *July 26, Philadelphia Business Journal* — **ID theft investigations tie into major banks.** Federal prosecutors in Philadelphia Wednesday, July 26, charged 24 people in connection with six separate identity theft schemes, two of which involved mortgage fraud. In one indictment, 10 defendants were charged with using personal information of hundreds of bank customers to cash counterfeit checks and withdraw money from customer accounts. U.S. Attorney Patrick Meehan said Charles White, 38, and Allen Smith, 30, both of Philadelphia, led a group of 10 defendants in conspiring to use the names, Social Security numbers, addresses and birth dates of potentially hundreds of customers of Commerce Bank, Wachovia Bank, PNC Bank, and M&T Bank. Between February 2004 and November 2005, Meehan said the group cashed closed−account foreign checks at drive−up teller windows at Commerce, cashed counterfeit checks inside Wachovia and withdrew funds from customer accounts at Wachovia, M&T and PNC banks. The defendants are charged with aggravated identity theft, bank fraud and related offenses.
Source: http://www.bizjournals.com/philadelphia/stories/2006/07/24/d aily30.html?from_rss=1

12. *July 26, Associated Press* — **Navy computers with personal data stolen.** Two laptop computers with personal information on about 31,000 Navy recruiters and their prospective recruits were stolen from Navy offices in New Jersey in June and July, the Navy disclosed on Wednesday, July 26. "There have been no reports of illegal usage of personal data identified by these incidents," said Navy spokesperson, Lt. Bashon W. Mann, adding that the Navy is identifying the affected individuals. He said the information on the laptops was secured by several layers of password protection. One laptop was reported stolen from a recruiting station in Trenton, NJ, in early June, and the other was taken from a Jersey City, NJ, recruiting station in early July. Information on the computers included a list of applicants and recruiters as well as information from selective service and school lists. About 4,000 included Social Security numbers. The police and the Navy Criminal Investigative Service are investigating.
Source: http://www.chron.com/disp/story.mpl/ap/politics/4074633.html

13. *July 25, Viruslist* — **Cybercrime in Spain on the rise.** Online fraud in Spain experienced a year−on−year growth of 50 percent in the first four months of 2006, according to Victor Domingo of the Internet Users Association. Over the past 18 months some 500 bogus websites of banks and other financial institution used in phishing attacks have been detected. In all, 206

massive phishing attacks on Spanish financial institutions were seen in 2005. The Spanish Ministry of Industry, Tourism and Trade has launched a new initiative to stop online fraud by informing Internet users of the dangers and how they can protect themselves. The government has timed this campaign against fraud specifically to target those Internet users who will be online more often than normal due to the summer holidays.
Source: http://www.viruslist.com/en/news?id=192384669

[Return to top]

Transportation and Border Security Sector

14. *July 27, Boston Globe* — **Boston commuter rail problems prompt a showdown.** The head of the Massachusetts Bay Transportation Authority (MBTA) met Thursday, July 27, with officials from the Massachusetts Bay Commuter Railroad who run the T's (transit) commuter trains to complain about abysmal on−time performance and unhelpful employees and to call for quick improvements on stifling−hot coaches, failing equipment, and late or canceled trains. It is the most serious conflict yet between the MBTA and the commuter railroad. The meeting was so important that T officials said the head of the commuter rail consortium was summoned from vacation. While subways, ferries, and buses are handling a surge in passengers since the fatal collapse July 10 of a Big Dig tunnel ceiling and subsequent road closings, commuter rail service is worsening, Daniel A. Grabauskas, the T's general manager, said. The 13 commuter rail lines serve about 140,000 passengers on an average weekday, but that number has increased since the Big Dig closings. Equipment shortages appear to be a key problem for the commuter railroad, which on Monday had 24 of 80 locomotives in the shop for service or maintenance, above the maximum of 20 that the contract with the MBTA allows.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/07/27/commuter_rail_snags_prompt_a_showdown/

15. *July 27, Associated Press* — **Northwest flight makes emergency landing in Michigan.** Smoke began filling a Toronto−bound Northwest Airlines plane with 82 passengers and five crewmembers aboard, forcing it to make an emergency landing in central Michigan, an airline spokesperson said. Flight 884 made a safe landing at MBS International Airport in Freeland, MI, 80 minutes after it left Minneapolis−St. Paul International Airport, said Northwest spokesperson David Rivard. A crew made repairs and the plane left for Toronto International Airport about 11:20 p.m. CDT, Rivard said. The smoke entered the cabin because of a minor problem with a fan, Rivard said.
Source: http://www.usatoday.com/travel/flights/2006−07−27−northwest− landing_x.htm

16. *July 27, Associated Press* — **"Human error" caused cruise ship tilt.** Human error caused a cruise ship to tilt abruptly at sea last week, sending furniture and debris flying about the vessel and injuring passengers, a cruise line official has said. Though federal investigations continue, the official, Alan Buckelew, president of Princess Cruises, wrote in a letter to passengers that "the incident was due to human error and the appropriate personnel changes have been made." Shortly after departing Port Canaveral last week, the ship, the Crown Princess, tilted an estimated 16 to 18 degrees, tumbling passengers, chairs, tables and other objects, and seriously injuring at least 20 people.
Source: http://www.nytimes.com/2006/07/27/us/27brfs−003.html?ref=us

17. *July 26, Department of Transportation* — **FRA announces national discussion on improving safety at private highway−rail grade crossings.** The Federal Railroad Administration (FRA) will hold a series of public meetings across the country beginning in August to start a national discussion on the challenging issue of improving safety at the nation's largely unregulated private highway−rail grade crossings, FRA Administrator Joseph H. Boardman announced. Establishing responsibility for safety at private crossings is one of the primary goals of the U.S. Department of Transportation's Highway−Rail Grade Crossing and Trespass Prevention Action Plan issued in 2004, Boardman said. Private crossings are owned by private property owners who allow roadway access over railroad tracks to residential, commercial, or agricultural areas not meant for general public use, Boardman explained. Each year, about 400 accidents, and between 30 and 40 fatalities, occur at the over 94,000 private crossings used by both freight and passenger trains, he stated. The FRA is seeking comments on topics such as determining when a private crossing has a public purpose and whether the State or Federal government should assume a greater role in setting safety standards. The first public meeting will be held in Fort Snelling, MN, with others tentatively planned for North Carolina, California, and Louisiana later this year.
Source: http://www.dot.gov/affairs/fra0806.htm

18. *July 26, Government Accountability Office* — **GAO−06−821: Rail Transit: Additional Federal Leadership Would Enhance FTA's State Safety Oversight Program (Report).** The U.S. rail transit system is a vital component of the nation's transportation infrastructure. Safety and security oversight of rail transit is the responsibility of state−designated oversight agencies following Federal Transit Administration (FTA) requirements. In this report, the Government Accountability Office (GAO) addressed: (1) how the State Safety Oversight program is designed; (2) what is known about the program's impact; and (3) challenges facing the program. We also provide information about oversight of transit systems that cross state boundaries. To do our work we surveyed state oversight agencies and transit agencies covered by FTA's program. GAO is recommending that the Secretary of Transportation direct FTA to (1) set performance goals for the program and develop a plan for maintaining the stated schedule of auditing oversight agencies and (2) develop and encourage completion of a recommended training curriculum for oversight agency staff. Also, we recommend that the Secretary of the Department of Homeland Security (DHS) direct the Assistant Secretary of the Transportation Security Administration (TSA) to coordinate their security oversight activities and audits with FTA and transit and oversight agencies. FTA and TSA generally concurred with the report and are considering how to implement the recommendations.
Highlights: http://www.gao.gov/highlights/d06821high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−821

19. *July 26, WPMI (AL)* — **Vandals destroy airport runway lights.** Hoping to find the person or persons responsible for vandalizing several runway lighting systems at Brookley Field in Mobile, AL, the FBI is now offering a $5,000 reward for information leading to an arrest. The incident, which reportedly happened the last week of April, caused severe damage to lights associated with the instrument landing system −− critical for pilots landing their airplanes in bad weather. The FBI's anti−terrorism task force is also looking into the incident. Authorities say whoever committed the crime may have gained entry to the runway through several fences down because of Hurricane Katrina. Authorities aren't sure if juveniles or adults are responsible

for this crime. Brookley Field is used by a mix of private, corporate, military, and cargo aircraft, including FedEx and UPS.
Source: http://www.wpmi.com/news/local/story.aspx?content_id=CF7A93C8-3398-4D9C-9642-34038E8DA11C

[Return to top]

Postal and Shipping Sector

20. *July 27, Associated Press* — **FedEx plane goes off Kentucky runway.** A FedEx Corp. 727 cargo plane went off the runway at Louisville International Airport Thursday, July 27, after the pilot aborted the takeoff, airport officials said. The plane with a crew of three was scheduled to fly to Memphis, TN, where the company is based. FedEx officials said they had no details about the accident. Federal Aviation Administration spokesperson Les Dorr said it wasn't immediately clear why the pilot stopped the takeoff.
Source: http://www.boston.com/news/nation/articles/2006/07/27/fedex_plane_goes_off_ky_runway/

21. *July 27, Government Accountability Office* — **GAO-06-733: U.S. Postal Service: Delivery Performance Standards, Measurement, and Reporting Need Improvement (Report).** U.S. Postal Service (USPS) delivery performance standards and results, which are central to its mission of providing universal postal service, have been a long-standing concern for mailers and Congress. Standards are essential to set realistic expectations for delivery performance and organize activities accordingly. Timely and reliable reporting of results is essential for management, over-sight, and accountability purposes. The Government Accountability Office (GAO) was asked to assess (1) USPS's delivery performance standards for timely mail delivery, (2) delivery performance information that USPS collects and reports on timely mail delivery, and (3) progress made to improve delivery performance information. GAO recommends that USPS take actions to modernize its delivery standards, implement delivery performance measures for major types of mail by providing clear commitment and more effective collaboration, and improve the transparency of delivery performance standards, measures, and results. In commenting on a draft of this report, USPS disagreed that its standards are outdated and detailed its vision to improve service measures and transparency. USPS did not directly comment on three of GAO's four recommendations. On GAO's transparency recommendation, USPS said that its standards should be more visible and is exploring providing more of this information.
Highlights: http://www.gao.gov/highlights/d06733high.pdf
Source: http://www.gao.gov/cgi-bin/getrpt?GAO-06-733

[Return to top]

Agriculture Sector

22. *July 27, Chronicle Herald (Canada)* — **Hog-wasting disease blow to farms across Nova Scotia.** Nova Scotia, Canada, pork producers are battling a crippling hog disease that is wasting away their herds and adding to their troubling financial woes. While the world scrambles to

find a vaccine for post−weaning multi−systemic wasting syndrome (PMWS), Nova Scotia pork producers are asking for provincial aid to help offset their losses. "We are very concerned about the impact of this disease on Nova Scotia farms," Pork Nova Scotia chairman Martin Porskamp said in a letter to Agriculture Minister Brooke Taylor marked urgent. "We have had reports of death losses of 20 to 40 per cent during an outbreak. These farmers simply cannot survive this kind of economic loss, especially during a period of prolonged low price," wrote Porskamp, a Kings County hog producer. Pork Nova Scotia, estimates the economic impact of the disease from 2002 to 2006 at $1.3 million, with a projected impact for 2007 of $554,356.
PMWS information: http://www.thepigsite.com/diseaseinfo/86/post−weaning−multisystemic−wasting−syndrome−pmws
Source: http://thechronicleherald.ca/NovaScotia/518202.html

23. *July 27, Agricultural Research Service* — **Lab on path to new Marek's disease vaccine.** Experimental versions of the first genetically engineered Marek's disease vaccine for poultry are being developed by Agricultural Research Service (ARS) scientists in Michigan. Scientists at the ARS Avian Disease and Oncology Laboratory are testing the vaccines with an eye toward producing the next−generation vaccine against Marek's disease. These recombinant DNA vaccines should provide protection longer than previous versions of the vaccine, possibly buying the time needed to breed the first generation of Marek's−resistant chickens, using other modern genetic techniques. Since the lab's founding in the 1930s, scientists there have held the tumor−causing Marek's disease in check. In 1972, ARS scientists developed the first vaccine against Marek's, as well as several updates as the disease evolved. It's still a major threat to the poultry industry, because new strains continue to emerge to challenge the current vaccine. The researchers are also breeding chickens resistant to Marek's and other diseases, using the chicken genome map and other genetic tools.
Marek's disease information: http://www.addl.purdue.edu/newsletters/2005/Spring/mareks.ht m
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

24. *July 26, Stop Soybean Rust News* — **First soybean rust found on soybeans in Louisiana.** The first Asian soybean rust on soybeans in Louisiana this year was confirmed in Rapides Parish Wednesday, July 26. This is the farthest west in the United States that soybean rust is active at the moment, and the northern−most point in Louisiana with rust. Currently, rust has been found on this year's soybeans in six counties in Alabama, Florida, Georgia and Louisiana. The rest of the finds have been on kudzu. A total of 26 counties have reported rust this year and include five in Alabama, 12 in Florida, five in Georgia, three in Louisiana, and one in Texas.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=891

[Return to top]

Food Sector

25. *July 26, Reuters* — **Safeguards vastly cut mad cow disease risk to people.** The U.S. government virtually eliminated the threat of mad cow disease to consumers by requiring the removal of brains, spinal cords and other high risk items from older cattle, the Harvard Center for Risk Analysis said on Tuesday, July 25. Mad cow disease is a fatal, brain−wasting disease believed to be spread by contaminated feed. People can contract a human version of the disease by eating tainted meats. "Removing high risk tissues, often called specified risk materials

(SRMs), from animals over 30 months of age almost completely eliminates potential human exposure," the center said in an update to its 2003 study, commissioned by U.S. Department of Agriculture (USDA). In its report, the center said two other USDA measures −− banning "downer" cattle too ill to walk and the use of so−called advanced meat recovery equipment −− also were helpful but to a lesser degree than SRM removal.
Risk Analysis of Transmissible Spongiform Encephalopathies in Cattle And the Potential for Entry of the Etiologic Agent(s) Into the U.S. Food Supply:
http://www.hcra.harvard.edu/pdf/madcow_report.pdf
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006−07−26T163934Z_01_COL659845_RTRUKOC_0_US−BSE− RISK.xml

26. *July 25, Reuters* — **Major food crisis looms in Lebanon.** A major food crisis is looming in Lebanon, where fighting between Israeli forces and Hezbollah has destroyed roads and bridges and forced people to abandon their crops, the United Nations food agency said on Tuesday, July 25. Insecurity and damaged infrastructure have interrupted the food supply chain in a country that relies on imports for around 90 percent of its cereal needs, the Food and Agriculture Organization (FAO) said. What little is produced on the ground is also likely to be affected because some of the crops are in areas where fighting is taking place. Lebanon depends heavily on imports of essential food items like wheat, rice, sugar and milk powder.
Source: http://www.alertnet.org/thenews/newsdesk/L2543635.htm

[Return to top]

Water Sector

27. *July 27, Union Leader (NH)* — **Exeter water doesn't meet arsenic standards.** Exeter, NH's water supply is failing to meet federal arsenic standards, according to the New Hampshire Department of Environmental Services (DES). Town officials were notified of the shortfall by DES in a letter dated July 14. Town Manager Russell Dean said the problem stems from changes in federal arsenic regulations. Before June 2006, a municipal water supply could have arsenic levels of 50 parts per billion. In January, the government lowered the acceptable level to 10 parts per billion. Tests conducted in June show Exeter's water supply with an arsenic level of 11 parts per billion.
Source: http://www.unionleader.com/article.aspx?headline=Exeter+water+doesn%27t+meet+arsenic+standards&articleId=14a208d6−70dd−4a95−a853−8e56d0c3b179

[Return to top]

Public Health Sector

28. *July 27, Associated Press* — **Rare disease reported in transplants.** Two U.S. heart transplant patients who died earlier this year had contracted a parasitic tropical disease from their new organs, health officials reported Thursday, July 27. The two California men are the fourth and fifth U.S. patients believed to have been infected with Chagas' disease through organ transplants, according to the U.S. Centers for Disease Control and Prevention (CDC). Organ

donors are screened for Chagas' in South America, where the disease is much more common. No screening test for Chagas' is licensed in the U.S. The two men, ages 64 and 73, died at separate Los Angeles hospitals after being treated with Chagas'−fighting drugs from a special CDC stockpile of medicines not available in this country. The infected organs came from one person born in Central America and another who had traveled to Mexico. In 2001, the CDC reported three cases of Chagas' in three U.S. women who had received organs from an immigrant from Central America. Doctors presumed the donor was infected, but no specimens were available for testing. About 12 million people in Central and South America are infected with Chagas', but only 100,000 U.S. residents have it, according to rough estimates.
Chagas disease information: http://www.cdc.gov/ncidod/dpd/parasites/chagasdisease/default.htm
Source: http://news.yahoo.com/s/ap/20060727/ap_on_he_me/transplant_infections;_ylt=Am2YJXIdqa9n.0o.IyOG3D3VJRIF;_ylu=X3oDMTA2Z2szazkxBHNlYwN0bQ−−

29. *July 26, Reuters* — **No easy fix for emergency rooms, experts say.** A lack of staff, space and equipment hobbles the U.S. emergency medical system and almost no steps have been taken to improve things despite numerous warnings, emergency room professionals told Congress on Wednesday, July 26. But emergency room physicians and members of Congress alike were at a loss about what to do to fix a system that almost everyone agrees is at a breaking point. "It isn't too clear and that is because what is required is so big," Rick Blum, an emergency room doctor from West Virginia who is president of the American College of Emergency Physicians, said in an interview. A subcommittee of the House of Representatives Homeland Security Committee held the hearing to ask if there was anything the federal government could do to address the problems. So what happens if pandemic influenza comes, or someone sets off a biological weapon, or giant earthquakes or hurricanes hit? "We are neither prepared nor capable of responding," Washington Republican Rep. Dave Reichert, chairman of the House of Representatives Subcommittee on Preparedness, Science and Technology, told the hearing.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006−07−26T212906Z_01_N26302778_RTRIDST_0_HEALTH−EMERGENCY−DC.XML

30. *July 26, Agence France−Presse* — **Asian countries to meet in India on bird flu.** Officials from 11 Asian countries will meet in New Delhi, India, for two days starting Thursday, July 27, to discuss bird flu control and worst−case scenario preparations, a World Health Organization (WHO) official said. "The secretary−level meeting will take place tomorrow," said Harsaran Bir Kaur Pandey, spokesperson for the WHO Southeast Asia regional office. "The day after will be the ministerial−level meeting." Ministers from the health or agriculture departments of Afghanistan, Bangladesh, China, India, the Maldives, Myanmar, Nepal and Sri Lanka are expected to attend. Officials representing Bhutan, Indonesia and Thailand will also be in New Delhi to take part in the working meeting Thursday. Senior officials from the WHO, the Food and Agriculture Organization and the World Organization for Animal Health (OIE), the three main international bodies spearheading the efforts to control bird flu will attend as well. The meeting in New Delhi will focus on preparing for a pandemic, animal husbandry issues and on how to improve communication with local communities.
Source: http://news.yahoo.com/s/afp/20060726/hl_afp/healthfluindiawho_060726170724;_ylt=AiuTqNkWfTIRM1s4sYo2W1mJOrgF

[Return to top]

Government Sector

31. *July 27, Government Accountability Office* — **GAO−06−1012T: Homeland Security: Challenges in Creating an Effective Acquisition Organization (Testimony).** The Department of Homeland Security (DHS) has some of the most extensive acquisition needs within the U.S. government. In fiscal year 2005, the department reported that it obligated almost $17.5 billion to acquire a wide range of goods and services. DHS ‘s acquisition portfolio is broad and complex, including procurements for sophisticated screening equipment for air passenger security; technologies to secure the nation’s borders; trailers to meet the housing needs of Hurricane Katrina victims; and the upgrading of the Coast Guard’s offshore fleet of surface and air assets. This testimony summarizes the Government Accountability Office’s (GAO) reports and testimonies, which have reported on various aspects of DHS acquisitions. It addresses (1) areas where DHS has been successful in promoting collaboration among its various organizations, and (2) challenges it still faces in integrating the acquisition function across the department; and (3) DHS’ implementation of an effective review process for its major, complex investments. The information in this testimony is based on work that was completed in accordance with generally accepted government auditing standards.
Highlights: http://www.gao.gov/highlights/d061012thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−1012T

32. *July 27, USA TODAY* — **Threats up against federal judges.** Threats against federal judges and other court employees have reached record numbers, the U.S. Marshals Service says. The number of threats in fiscal year 2005 increased 63 percent from 2003. "It seems like every few months there's some type of major threat to a judge," says U.S. Marshals Service Director John Clark. "It's very clear to me that we need to continue to be vigilant." The Marshals Service, charged with protecting federal judges, prosecutors, jurors and other court employees, has tripled its number of threat investigators and analysts from eight to 25 to respond to the threats, says Donald Horton, chief inspector for the marshals' Office of Protective Intelligence. He attributes the increase in threats to more litigation, more aggressive communication from people with complaints against judges, easier access to judges' information and improved reporting of threats. Recent high−profile shootings have drawn national attention to judicial security and underscored weaknesses in judicial protection. Congress has responded by approving nearly $12 million to install security systems at judges' homes. Congress also is considering other security proposals, including tougher criminal penalties for people convicted of threatening judges. State judges, who are not under the marshals' protection, also are vulnerable.
Source: http://www.usatoday.com/news/nation/2006−07−26−judges−cover_x.htm

[Return to top]

Emergency Services Sector

33. *July 27, Detroit Free Press (MI)* — **Michigan officers train for attacks on water.** In Michigan, members of the Wayne County Sheriff's Special Response Team (SRT) and Marine

Unit joined on the Detroit River to train for potential water attacks. With more than 30 miles of international shoreline −− along with chemical, water−treatment and electrical power plants in Wayne County −− Sheriff Warren Evans wanted to increase preparedness for any water−based assaults. Deputies were able to determine whether they had the ability to get in and out of boats with ease, scuba dive and navigate the waters in heavy gear and equipment while still protecting their weapons. "The units performed well together, but a lot of simple issues came up that you would have not thought of in the boardroom, but get practically worked out when you're in the field," Evans said.
Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20060727/NEWS02/607270435/1004/NEWS

34. *July 26, WAVE3−TV (KY)* — **Floyd County, Indiana stages drill to test readiness.** Medical and emergency officials in Floyd County, IN set out to determine how well they were prepared on Wednesday, July 26 with a disaster drill designed to test Floyd Memorial Hospital's new procedures and equipment in the face of a chemical disaster. According to Floyd Memorial's Manager of Emergency Services, Kathy Scifres, the hospital has dealt with chemical exposure incidents before. In the drill, the victims were "exposed" to chlorine, with varying degrees of exposure and injury. Their conditions were quickly assessed by an emergency team, with any chemical exposure issues addressed in a new, state of the art, decontamination unit. According to hospital officials, the new decontamination unit, and the hospital's plan, passed the first test, although there were a few areas for improvement. As Dr. Tom Harris explains, "we had the usual problems with trying to assess people at the scene, knowing what was coming in so that we were prepared to start out with. It's always a learning process but we feel a lot more confident now."
Source: http://www.wave3.com/global/story.asp?s=5201709

35. *July 26, South Bend Tribune (IN)* — **Airport drill keeps Indiana departments prepared.** In Indiana, the Berrien County Fairgrounds and Andrews University Airpark housed the fourth annual county emergency training drill on Tuesday, July 25. The drill was for 13 different fields, including fire departments, police departments, sheriff's deputies, departments of public works, departments of transportation, Emergency Medical Services crews, paramedics and more from across Berrien County. Firefighters had the opportunity to practice aircraft rescue firefighting on an aircraft training simulator and had to work in teams to extinguish controlled flames surrounding the aircraft to create a safe path to the plane and complete the drill. Next, the firefighters were trained to carry aircraft crew and passengers out of the plane to safety. While emergency crews tested their response abilities, the Red Cross was able to practice a mass feeding in a disaster situation; Berrien Springs Middle School and Blossomland Learning Center also took advantage of the drill to practice their evacuation plans. The bomb squad was also put to the test. Members were able use their new robot, which is fully equipped with fiber−optic live video feed from three cameras.
Source: http://www.officer.com/article/article.jsp?id=31790&siteSect ion=1

36. *July 26, Honolulu Advertiser (HI)* — **Hawaii treating Daniel as serious.** The storm that was Hurricane Daniel weakened on Tuesday, July 25 to a tropical depression, but the Hawaii's emergency response agencies continued preparations for the possibility of flooding on the Big Island −− and using the event as a statewide preparedness exercise. "It's almost totally dissipated, but there's still a lot of moisture in it," said Jim Weyman, director of the Central

Pacific Hurricane Center. "It could be like Kenneth last year, when we got quite a bit of rain and some flooding." Hurricane Kenneth had dissipated to a tropical depression when it reached the Big Island on September 30, but it still caused flash floods on several islands. The Big Island could see significant rainfall from Daniel starting late morning Friday, July 21. State highway crews positioned equipment around the island so that the right gear will be available where needed, arranged for spare fuel and checked light stands in the event night work is required, said Stanley Tomura, district highways engineer with the state Department of Transportation. Along county roads, crews cleared drains and streams, checked emergency equipment and counted the number of sandbags on hand in each district, said county public works chief Bruce McClure.
Source: http://the.honoluluadvertiser.com/article/2006/Jul/26/ln/FP6 07260362.html

[Return to top]

Information Technology and Telecommunications Sector

37. *July 27, Reuters* — **FCC: U.S. broadband subscribers jump 33 percent in 2005.** U.S. high−speed Internet subscriptions soared 33 percent last year to 50.2 million lines, according to the latest data released by the Federal Communications Commission (FCC) Wednesday, July 26. More consumers signed up for digital subscriber line (DSL) service from telephone companies like AT&T Inc. and Verizon Communications Inc. than cable modem service from companies like Comcast Corp. and Time Warner Inc. DSL subscriptions jumped 5.7 million lines versus cable companies adding 4.2 million subscribers in 2005, according to the FCC. The cable industry's market share dropped 3.5 percentage points to 57.5 percent while DSL gained 3.3 percentage points to reach 40.5, the agency said.
Source: http://www.eweek.com/article2/0,1895,1995061,00.asp

38. *July 27, VNUNet* — **Microsoft to push IE 7 as "high priority" update.** Microsoft plans to distribute its forthcoming Internet Explorer 7 (IE) browser as a "high priority" upgrade through its automatic Windows Update service, group program manager Tony Chor said in a posting on the IE Blog. The application will automatically download as a background process or when users run the auto update service to download and install security updates. This method of distribution through the auto update service is considered aggressive and is likely to result in the majority of users proceeding to install the application. But the approach could lead to compatibility issues. Internet Explorer 7 requires developers of some online applications to change their code to ensure that it works in the new browser.
Source: http://www.vnunet.com/vnunet/news/2161140/microsoft−push−ie7 −priority

39. *July 27, Register (UK)* — **United States cedes control of the Internet.** In a meeting that will go down in Internet history, the United States government Wednesday night, July 26, conceded that it can no longer expect to maintain its position as the ultimate authority over the Internet. Having been the Internet's instigator and, since 1998, its voluntary taskmaster, the U.S. government finally agreed to transition its control over not−for−profit Internet overseeing organization Internet Corporation for Assigned Names and Numbers, making the organization a more international body. However, assistant commerce secretary John Kneuer, the U.S. official in charge of such matters, also made clear that the U.S. was still determined to keep control of the net's root zone file −− at least in the medium−term.

Source: http://www.theregister.co.uk/2006/07/27/ntia_icann_meeting/

40. *July 26, NTA−Monitor* — **Cisco VPN concentrator IKE resource exhaustion denial−of−service advisory.** There is a vulnerability in Cisco VPN which affects Phase−1 of the IKE protocol. Both Main Mode and Aggressive Mode over both UDP and TCP transports are affected. Analysis: The vulnerability allows an attacker to exhaust the IKE resources on a VPN concentrator by sending a high rate of IKE requests, which will prevent valid clients from connected or re−keying. The attack does not require a high bandwidth, so one attacker could potentially target many concentrators.
Affected Versions: The issue is believed to affect all models of Cisco VPN 3000 Concentrator: 3005, 3015, 3020, 3030, 3060 and 3080. It is suspected that other Cisco products that support IKE may also be affected, but this has not been confirmed.
Solution: There is no known fix or workaround at this time.
Source: http://www.nta−monitor.com/posts/2006/07/cisco−concentrator− dos.html

41. *July 25, eWeek* — **Bugle goes Googling for source code flaws.** The world's most popular search engine can be used to pinpoint software security bugs in source code available on the Internet, according to a new research project launched by a UK−based researcher. The project, called Bugle, is a collection of Google search queries that can be used to identify some of the most common vulnerabilities in open−source code indexed by the search giant. Emmanouel Kellinis, a security penetration tester and source code reviewer for KPMG in London, started working on Bugle privately to find pinpoints to some of the most common coding mistakes and decided to go public with the project to expand the list of search queries. Kellinis believes security researchers can combine Bugle queries with Google's "highly intelligent indexing algorithms" to identify vulnerable code indexed by the search engine. "Bugle will give you hints for a potential vulnerability, but you still require skill to identify an actual issue," he explained.
Source: http://www.eweek.com/article2/0,1895,1994003,00.asp

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 has received information that a website on the Internet is hosting malicious software that has been or is currently being used to compromise systems.

IP: 211.34.248.244

Activity:
This activity is similar to what was reported on July 6th concerning the “beststartmotor” domain. The original email stated: “In April 2006, users reported

having their web browsers redirected from other websites to the domain beststartmotor.com using an HTML command called an iframe. Once redirected, the victim's web browsers usually download malware onto the victim's computer." Currently, another website may have a similar iframe link to IP 211.34.248.244. Once a web browser on a victim system follows this link, the victim computer may download malware which can compromise that computer.

Recommendation:
US−CERT suggests that each agency evaluate the potential risk and take protective measures in a manner that is consistent with the agency's policies and procedures. Please refrain from investigating / visiting the IP address as this may result in accidental infection of your computer. Please be advised that the IP address listed above may also host additional domains and websites. However, this information is being shared to allow the GFIRST community to understand the potential risk associated with those domains.

US−CERT requests that all agencies examine firewall, web proxy and other network perimeter device logs for suspicious traffic to and from the above IP. Should you encounter such activity, please notify US−CERT at soc@us−cert.gov or via phone at 888−282−0870.

Active Exploitation of a Vulnerability in Microsoft PowerPoint
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 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

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

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 6881 (bittorrent), 38566 (−−−), 7200 (fodms), 445 (microsoft−ds), 80 (www), 24232 (−−−), 113 (auth), 135 (epmap) 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 or visit their Website: www.us−cert.gov.

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

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