Department of Homeland Security Daily Open Source Infrastructure Report for 01 August 2007

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

Daily Highlights

- Senators Richard Burr and Susan Collins have drawn up legislation −− called the National Agriculture and Food Defense Act −− with the goal of creating a national strategy to prepare for, detect, respond to and recover from an agro−terror attack or catastrophic food emergency. (See item 17)
- Reuters reports a U.S. delegation has arrived in Beijing on a five−day fact−finding mission concerning food and drug safety amid a series of health scares about the "made in China" label, affecting items from pet food to poisonous ingredients in exports of toys, toothpaste, and fish. (See item 18)

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 31, Associated Press* — **Utilities search for buried danger.** For years, scientists at utilities around the country have tried to peer deep into their cities without jackhammers. They've experimented with robotic probes, ground−penetrating radar, and thermal cameras. After a morning of downpours on the day of the Manhattan steam blast, Consolidated Edison Co. resorted to an old−fashioned method for identifying spots where hot pipes had come into potentially dangerous contact with cold rainwater: It sent employees out in trucks to look for

manhole steam. That system didn't detect anything amiss. Hours later, a steam main near Grand Central Terminal exploded, creating a colossal geyser that swallowed a truck, tore a 25−foot−deep crater in the street, burned bystanders and showered the neighborhood with toxic debris. Con Edison isn't the only utility now turning to higher−tech methods of trying to find problems in the country's aging infrastructure. The Trigen Companies, which operates steam systems in 11 cities, including Boston, Philadelphia and Las Vegas, said it occasionally flies thermal cameras over its networks, looking for heat plumes that might indicate a steam leak, or pooling groundwater in the area of a pipe.
Source: http://hosted.ap.org/dynamic/stories/M/MANHATTAN_EXPLOSION?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

2. *July 30, USA TODAY* — **Gas prices at the pump fall but oil rises.** Oil prices flirted with record highs Monday, July 30, and continued to rise Tuesday, while gasoline prices fell for a second consecutive week, as oil and gas prices continue to uncharacteristically move in opposite directions. Gas prices may decline further in coming weeks as the unusual disconnect between oil and gasoline prices continues. The nationwide average price of a gallon of regular gasoline was $2.876 Tuesday, down more than eight cents from a week earlier and 34 cents below the recent high seen on May 21, the Department of Energy said. Average prices were under $3 a gallon in 36 states, according to a separate survey from Oil Price Information Service and motorist club AAA. Strong demand for oil from refineries that are coming back online after being down for maintenance earlier this year is leading to higher prices for oil, Alaron Trading oil analyst Phil Flynn says. The higher oil costs are not expected to lead to increased prices at the gasoline pump. Kloza expects prices to continue to fall in the next week as retail prices catch up with recent declines in wholesale gasoline costs.
Source: http://www.usatoday.com/money/industries/energy/2007−07−30−oil−prices_N.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *July 30, Associated Press* — **Evacuations ordered after spill at chemical plant.** A chemical spill in Louisville, KY, Monday morning, July 30, prompted authorities to order evacuations of a nearby area. Louisville Fire and Rescue responded to the report of a chemical spill at Chemcentral. A chemical widely used in dry−cleaning and metal degreasing operations (perchloroethylene) spilled in a concrete containment area at the business. Metro Safe reports no hospital runs were made from the scene.
Source: http://www.newschannel5.com/Global/story.asp?S=6858990&nav=menu374_2_4

[Return to top]

Defense Industrial Base Sector

4. *July 31, Government Accountability Office* — **GAO−07−711: Stabilizing Iraq: DoD Cannot Ensure That U.S.−Funded Equipment Has Reached Iraqi Security Forces (Report).** Since 2003, the United States has provided about $19.2 billion to develop Iraqi security forces. The Department of Defense (DoD) recently requested an additional $2 billion to continue this effort.

Components of the Multinational Force−Iraq (MNF−I), including the Multinational Security Transition Command−Iraq (MNSTC−I), are responsible for implementing the U.S. program to train and equip Iraqi forces. This report (1) examines the property accountability procedures DoD and MNF−I applied to the U.S. train−and−equip program for Iraq and (2) assesses whether DoD and MNF−I can account for the U.S.−funded equipment issued to the Iraqi security forces. To accomplish these objectives, the Government Accountability Office (GAO) reviewed MNSTC−I property books as of January 2007 and interviewed current and former officials from DoD and MNF−I. To help ensure that U.S.−funded equipment reaches Iraqi security forces as intended, GAO recommends that the Secretary of Defense (1) determine what DoD accountability procedures apply or should apply to the program and (2) after defining these procedures, ensure that sufficient staff, functioning distribution networks, and proper technology are available to meet the new requirements. DoD concurred with both recommendations.
Highlights: http://www.gao.gov/highlights/d07711high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−711

[Return to top]

Banking and Finance Sector

5. *July 31, Finjan* — **When Trojans go phishing.** Finjan, a developer of secure Web gateway products, released a report Tuesday, July 31, detailing how new crimeware is being used to steal banking customer data from infected PCs. During July 2007, Finjan has identified 58 criminals using the MPack toolkit who have successfully infected over 500,000 unique users. The infection ratio stands at 16 percent from 3.1 million attempts −− indicated by the Web traffic volumes of the infecting sites. Finjan’s analysis indicates that the crimeware being used within MPack steals bank account information, such as user name, password, credit card number, social security number etc., in a creative way. The crimeware is capable of stealing account information from several banks around the world without leaving any traces behind. Stolen data is being sent to the criminals over a secure communication channel to avoid detection. Users whose machines were infected by this crimeware will not notice any change to their normal PC and online browsing experience. The rootkit nature of the crimeware leaves no sign and does not impact the end−user experience. To compound the problem the crimeware downloaded by the MPack toolkit is still not detected by the majority of popular security products.
   Report (registration required): http://www.finjan.com/Content.aspx?id=1367
   Source: http://www.finjan.com/Pressrelease.aspx?id=1629&PressLan=123 0&lan=3

6. *July 31, Washington Post* — **Lost wallet's ID cards spawned mortgage fraud.** It was a little baffling when Jose F. Lara got a check in the mail for almost $2,800 from a bank in Arlington County, VA, in December. When the bank told him that it was the overpayment on his second mortgage, things got really baffling. He didn't have a second mortgage. Turned out it all tracked back to that day last year when Lara's wallet was stolen. Elizabeth Cabrera−Rivera found it and used Lara's identification to buy a house. A $419,000 townhouse in Springfield. With no money down. A townhouse she and her family moved into, refinanced and then quickly fled not long after Lara turned up at the bank in December. "They don't really see themselves as doing something wrong as long as they pay the bill," said Mari J. Frank, a California lawyer, identity

fraud victim and author of numerous books and articles on the subject. And Cabrera−Rivera had, in fact, been making the mortgage payments. Monday, July 30, Cabrera−Rivera, pleaded guilty in Arlington County Circuit Court to identity fraud, credit card theft, conspiracy and obtaining a loan under false pretenses.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/07/30/AR2007073001715.html

7. *July 30, InformationWeek* — **Four men plead guilty to using phony point−of−sale PIN−pad terminals to steal customers' data.** A finely tuned fraud−detection system earlier this year helped put the kibosh on a cross−country ring of payment−card thieves hitting up grocery stores in New England and stealing from ATMs in California. Now, four California men are facing several years in prison and fines for their roles in a skimming operation at Stop & Shop supermarkets that compromised more than 238 payment card account numbers and netted them more than $130,000. Mikael Stepanian, Arutyun Shatarevyan, Gevork Baltadjian, and Arman Ter−Esayan have all pleaded guilty to conspiracy to traffic in unauthorized access devices and aggravated identity theft for stealing credit and debit card account information in February through altered supermarket point−of−sale PIN−pad terminals they planted during overnight hours at four 24−hour Stop & Shop stores in Rhode Island and one in Massachusetts. The scam worked like this: As they entered a store, one of the men distracted a clerk while the others swapped the store's PIN−pad terminals with nearly identical devices that had been electronically altered to capture customers' account numbers and PINs. Several days later, the men returned to the store, replaced the original terminal, and made off with the altered one containing customers' account information.
Source: http://www.informationweek.com/software/showArticle.jhtml;jsessionid=NNKUQTKSCHZTUQSNDLPSKHSCJUNN2JVN?articleID=201201747&articleID=201201747

8. *July 30, RIA Novosti (Russia)* — **Russian hackers steal over $500,000 from Turkish banks.** Two un−named hackers from the Russian city of Togliatti on the Volga River stole over $500,000 over a period of two years from bank accounts in Turkey, Interior Ministry investigators said Monday, July 30. The two men purchased a dedicated server with remote access to a desktop hosted in a U.S. data center, and a special application capable of infecting banking computers in Turkey with a Trojan virus to obtain information on bank accounts, investigators said. One of the hackers has been arrested, and the other is on a federal wanted list. After processing the obtained information, the hackers transferred money to accounts of Turkish collaborators, who in turn cashed the money in and later transferred it to Togliatti via Western Union. The Interior Ministry's investigation committee said there were a total of 265 registered money transfers totaling $508,000 between February 2005 and April 2007.
Source: http://en.rian.ru/world/20070730/69939519.html

[Return to top]

Transportation and Border Security Sector

9. *July 31, Detroit Free Press* — **NWA calls back its pilots.** Northwest Airlines (NWA), which continues to lead its rivals in the percentage of flight cancellations, said Monday, July 30, that all of its remaining laid−off pilots have been asked to return and those who agree to come back

will be assigned training dates by Wednesday, August 1. Northwest has been calling back pilots as a way to curb the hundreds of cancellations that have plagued it in the past few days, as well as late last month. By Monday evening, the carrier had canceled 126 flights nationwide, including 39 in Detroit. Northwest spokesperson Roman Blahoski said that the airline began calling pilots back last August, when 700 were on furlough. He added that the pilot total through June 30 was 385. Air Line Pilots Association spokesperson Monty Montgomery said he didn't know how many accepted offers to return but said 37 pilots had resigned since they were called back. Another 48 pilots are being trained to return to work. Many laid−off pilots, who found other jobs during their furloughs, are delaying their return until they get a better idea of the airline's stability, Montgomery said. Northwest has blamed cancellations on pilot absenteeism, while pilots attributed the problem to crew shortages and an exhausted workforce.
Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20070731/BUSINESS06/707310370/1018

10. *July 31, DowJones/Associated Press* — **Airline industry optimism sapped by surging oil prices.** Whatever relief airlines hoped to receive from lower oil prices this winter is quickly disappearing. As the second−quarter reporting season wraps up, carriers have warned again that fuel, which is right up there with personnel as their biggest cost, is headed higher in the third and fourth quarters. That would put overall fuel costs for 2007 as high or even higher than they were in 2006. The forecasts include gains from locking in fuel prices through hedges, a strategy that gave Southwest Airlines a huge advantage over rivals during the first part of this decade but that can also backfire if prices go lower. "Rising fuel prices are a real concern in the second half," Thomas Horton, chief financial officer at American Airlines' parent AMR, told investors earlier this month. The largest U.S. carrier now anticipates shelling out $2.11 a gallon, on average, for fuel versus an average of $2.01 last year. A steep rise in crude−oil prices over the last two months has depressed shares in major carriers, despite a general trend toward improved profits.
Source: http://www.usatoday.com/travel/flights/2007−07−31−airline−fu el−costs_N.htm

11. *July 31, Government Accountability Office* — **GAO−07−1006: Border Security: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use (Report).** Travel documents are often used fraudulently in attempts to enter the United States. The integrity of U.S. passports and visas depends on the combination of well−designed security features and solid issuance and inspection processes. The Government Accountability Office (GAO) was asked to examine (1) the features of U.S. passports and visas and how information on the features is shared; (2) the integrity of the issuance process for these documents; and (3) how these documents are inspected at U.S. ports of entry. We reviewed documents such as studies, alerts, and training materials. We met with officials from the Departments of State, Homeland Security, and Commerce’s National Institute of Standards and Technology, and U.S. Government Printing Office, and with officials at seven passport offices, nine U.S. ports of entry, two U.S. consulates in Mexico, and two Border Crossing Card (BCC) production facilities. GAO recommends that State and DHS better plan for new generations of passports and visas, address potential vulnerabilities in the acceptance process of U.S. passport applications, utilize the electronic features of the new e−passport, better use the biometric feature of BCCs, and provide inspectors with systematic training prior to the issuance of new travel documents. State and DHS agreed with our recommendations.
Highlights: http://www.gao.gov/highlights/d071006high.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−1006

12. *June 29, Government Accountability Office* — **GAO−07−885: Airport Finance: Observations on Planned Airport Development Costs and Funding Levels, and the Administration's Proposed Changes in the Airport Improvement Program (Report).** To address the strain on the aviation system, the Federal Aviation Administration (FAA) has proposed transitioning to the Next Generation Air Transportation System (NextGen). To fund this system and to make its costs to users more equitable, the Administration has proposed fundamental changes in the way that FAA is funded. As part of the reauthorization, the Administration proposes major changes in the way that grants through the Airport Improvement Program (AIP) are funded and allocated to the 3,400 airports in the national airport system. In response, the Government Accountability Office (GAO) was asked for an update on current funding levels for airport development and the sufficiency of those levels to meet planned development costs. This report comprises capital development estimates made by FAA and Airports Council International (ACI), a leading industry association; analyzes how much airports have received for capital development and if sustained, whether it can meet future planned development; and summarizes the effects of proposed changes in funding for airport development. Airport funding and planned development data are drawn from the best available sources and have been assessed for their reliability. The Department of Transportation agreed with the findings of this report. This report does not contain recommendations.
Highlights: http://www.gao.gov/highlights/d07885high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−885

[Return to top]

Postal and Shipping Sector

13. *July 31, KDKA (PA)* — **Police warn about homemade explosives in mailboxes.** Three homemade explosives have turned up in mailboxes in Washington County, PA. One of them exploded in the community of Long Branch. Police say the bombs were made with a plastic water bottle, a plastic jug and a soda bottle filled with a blue liquid. They're warning residents not to handle the explosives −− just call police.
Source: http://kdka.com/local/local_story_212114430.html

14. *July 30, Associated Press* — **Inmate pleads guilty to mailing threatening letter in 2002.** A Kentucky prison inmate was sentenced to 21 months in prison for mailing a letter containing a white powder with a message that included the word “anthrax” to a federal office, prosecutors said Monday, July 30. Fred Luckenbill, 35, an inmate at Little Sandy Correctional Complex in Sandy Hook, was also sentenced to three years’ supervised release. Luckenbill admitted sending the letter to the U.S. District Court clerk in Louisville in September 2002 while he was an inmate at the Kentucky State Penitentiary in Eddyville. The envelope contained a white powder and a letter that said, “Death to all state and government officials, death to the United States, Anthrax,” U.S. Attorney David Huber’s office said in a statement. The clerk’s office was temporarily closed as a result of the mailing, but the powder was tested and found not to be hazardous, the statement said. Another inmate, Charles Harris, pleaded guilty in the same case and is to be sentenced October 15.
Source: http://www.whas11.com/news/local/stories/073007whasjdlocalle tters.c8a6d127.html

[Return to top]

Agriculture Sector

15. *July 30, Brownfield Ag News* — **More soybean rust reported in Arkansas and Texas.** The U.S. Department of Agriculture reports that Asian soybean rust was confirmed in Hempstead, Arkansas, the second finding in that state in a week. The rust was found in a sentinel plot at the South West Research and Extension Center in Hope. Hempstead is in southwest Arkansas, east of Little River County where rust was found Monday, July 23. Also, new cases of rust were confirmed on commercial beans in Bowie and Red River Counties in Texas.
Source: http://www.brownfieldnetwork.com/gestalt/go.cfm?objectid=17D536AA−ECED−FDBB−184D10F2280C5B99

16. *July 30, Ledger (FL)* — **Greening baffles scientists as it spreads through Florida.** While Florida citrus growers battled to eradicate citrus canker for nearly a decade, a far more dangerous, frightening threat, citrus greening, was lurking. It's more dangerous because the greening bacteria kill citrus trees every time. A tree can live with the canker bacteria, although the bacteria weaken the tree and lead to a significant drop in fruit production. So when federal and state officials halted the citrus eradication campaign in January 2006 after it destroyed more than 60,000 acres of commercial groves, growers accepted that they had to live with canker. They knew they had the caretaking tools to manage the disease. Greening is more frightening because even the state's top citrus researchers say they don't know enough about the disease to recommend any but the most basic control measures, such as removing infected trees. Without more effective controls, Florida citrus has a fight for survival against greening, which has destroyed commercial citrus operations in other countries once it became widespread. State and federal agriculture officials confirmed the first greening case in August 2005 in Homestead. As of July 16, it has spread to 110 commercial groves and 518 residential properties in 24 counties.
Source: http://www.theledger.com/article/20070730/NEWS/707300367/103 9

17. *July 30, Dairy Herd Management* — **Senate bill designed to protect food supply from terrorism.** Senators Richard Burr (R−NC) and Susan Collins (R−ME) have drawn up legislation with the goal of creating a national strategy to prepare for, detect, respond to and recover from an agro−terror attack or catastrophic food emergency. Called the National Agriculture and Food Defense Act, it would require federal departments to develop a coordinated strategy for agriculture and food emergency preparedness, as well as response and recovery plans. The bill outlines funding to train and educate state personnel on food defense tactics, as well as help states develop food emergency response plans. It also outlines ways to improve communication and coordination between state and federal authorities by authorizing states to hire agriculture and food defense liaison officers. The bill integrates nationwide diagnostic laboratory networks and develops on−site rapid diagnostic tools.
Source: http://www.dairyherd.com/news_editorial.asp?pgID=675&ed_id=6 697

[Return to top]

Food Sector

18. *July 31, Reuters* — **U.S. team heads for China to discuss food safety.** A U.S. delegation arrives in Beijing on Tuesday, July 31, on a five−day fact−finding mission on food and drug safety amid a series of health scares about the "made in China" label. The U.S. stepped up inspections of imports from China after a chemical additive in pet food caused the death of pets there this spring. Since then, poisonous ingredients have been found in Chinese exports of toys, toothpaste and fish, while the deaths of patients in Panama was blamed on improperly labeled Chinese chemicals that were mixed into cough syrup. "Our U.S. regulatory agencies are concerned about what they see as insufficient infrastructure across the board in China to assure the safety, quality and effectiveness of many products exported to the U.S.," the U.S. Department of Health and Human Services said in a statement. Following the mission, China and the United States would begin discussions to develop bilateral agreements on food and feed safety and on drug and medical device safety.
Source: http://www.reuters.com/article/healthNews/idUSPEK29771920070 731

19. *July 31, Associated Press* — **Copper theft spoils food bank groceries.** Thieves stole copper pipe from a freezer at Indiana's largest food bank, wasting nearly half a million dollars worth of food meant to help the poor, police said. The copper theft was captured by security cameras Friday night, July 27, police said, but the freezer's failure wasn't discovered until Monday. By then, thousands of pounds of groceries at the Gleaners Food Bank had become unusable. It was the third time in two months that copper had been taken from Gleaners. The food bank serves more than 300,000 people through more than 400 pantries and charities in 20 central Indiana counties. Copper can be sold for around $3 per pound, and thefts have become common across the country. In the food bank's case, it is unlikely the thieves got more than a few hundred dollars if they sold all the copper tubing to a scrap yard, Police Lt. Jeff Duhamell said.
Source: http://hosted.ap.org/dynamic/stories/F/FOOD_BANK_FREEZER?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

20. *July 30, New York Times* — **Without U.S. rules, biotech food lacks investors.** Federal officials seem to be getting serious about drafting rules that would determine whether and how bioengineered meat, milk and filets can safely enter the nation's food supply. Some scientists and biotechnology executives say that by having the U.S. Food and Drug Administration (FDA) spell out the rules of the game, investors would finally be willing to put up money to create a market in transgenic livestock. "Right now, it's very hard to get any corporate investment," said James Murray, a professor at the University of California, who developed goats with the infection−fighting milk. "What studies do you need to do? What are they looking for?" he said, referring to government regulators. "That stuff's not there." But some experts caution that, even if the FDA clears the regulatory path, investors might still shy away. Many fear that consumers would shun foods from transgenic animals. Critics say changing the genes of animals could lead to potentially harmful changes in the composition of milk or meat. They say there could also be risks to the environment if, for example, extra−large salmon were to escape into oceans and out−compete wild salmon for food or mates.
Source: http://www.nytimes.com/2007/07/30/washington/30animal.html?_r=2&ref=business&oref=slogin&oref=slogin

21.

July 29, U.S. Food and Drug Administration — **California Department of Public Health warns consumers not to eat ginger from China.** Mark Horton, director of the California Department of Public Health (CDPH), Sunday, July 29, warned consumers not to eat fresh ginger imported from China after the California Department of Pesticide Regulation's residue monitoring program detected the presence of aldicarb sulfoxide in some batches of imported ginger. Aldicarb sulfoxide is a pesticide that is not approved for use on ginger. The product is known to have been distributed to Albertson's stores and Save Mart stores in northern California by Christopher Ranch of Gilroy, CA. CDPH and the U.S. Food and Drug Administration are tracing the imported ginger from the importer (Modern Trading Inc. in Alhambra, California) to determine the full distribution of the product and to identify other retail stores that may have received the product. Currently, there are no reports of illness associated with the contaminated ginger. Ingestion of foods contaminated with aldicarb at low levels can cause flu−like symptoms (nausea, headache, blurred vision) which disappear quickly. However, at higher levels, ingestion of aldicarb contaminated food can also cause dizziness, salivation, excessive sweating, vomiting, diarrhea, muscle stiffness and twitching, and difficulty in breathing.
Source: http://www.fda.gov/oc/po/firmrecalls/cdph207_07.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

22. *July 31, Xinhua (China)* — **Vietnam reports new human bird flu case.** A 22−year−old woman from Vietnam's northern Ha Tay province was diagnosed as having bird flu, local newspaper Saigon Liberation reported Tuesday, July 31. The farmer, from the province's Thanh Oai district, is being treated in Bach Mai Hospital in Hanoi.
Source: http://news.xinhuanet.com/english/2007−07/31/content_6454846 .htm

23. *July 30, Xinhua (China)* — **Myanmar takes measure against bird flu outbreak.** Myanmar livestock authorities have taken measures to deal with a fresh bird flu outbreak in the country's southeastern Mon state early this week, sources with the Livestock Breeding and Veterinary Department (LBVD) said on Sunday, July 30. The measures included culling of over 300 chickens in two poultry farms where H5N1 virus was found. According to the LBVD, two poultry farms in Thanphyuzayat reported chickens dying abnormally on Tuesday, July 24, and after a series of testing for days, it was identified with H5N1. The renewed outbreak of H5N1 in the Mon state came a month after four new cases occurred at farms in three townships of Hmawby, Insein and Bago in June.
Source: http://english.people.com.cn/90001/90782/6226642.html

24. *July 30, Associated Press* — **Dengue fever rages across Asia.** Dengue fever is raging across Asia, prompting the World Health Organization to warn that the region could face the worst

outbreak of the mosquito−borne virus in nearly a decade. In Cambodia, the disease has attacked about 25,000 people and killed nearly 300 children this year. That's about three times more than the number of cases for all of 2005. Sick children have overwhelmed hospitals, forcing babies with fever to wait for beds outside with IV drips attached to their arms. Malaysia has seen a 50 percent jump in cases this year over the same period in 2006, with more than 1,000 patients admitted every week for the past month and 56 deaths recorded. In Indonesia, more than 100,000 infections have been reported this year, including 1,100 deaths. That compares to 114,000 cases and the same number of fatalities for all of 2006. The Singapore government has reported nearly 5,000 cases and at least three deaths. Early rains also caused a surge in cases in Thailand, with more than 20,000 cases reported through June, including 17 deaths. In Vietnam, health officials have seen a 40 percent increase over last year, reporting more than 33,000 infections this year and 32 deaths.
Source: http://www.forbes.com/feeds/ap/2007/07/30/ap3966847.html

[Return to top]

Government Sector

25. *July 31, Government Accountability Office* — **GAO−07−1149T: Capitol Visitor Center: Update on Status of Project's Schedule and Cost as of July 31, 2007 (Testimony).** Since the June 27, 2007, Capitol Visitor Center (CVC) hearing, the project's construction has progressed, and according to the latest schedule, Architect of the Capitol (AOC) is still projecting a June 27, 2008, completion date and a September 22, 2008, opening date. Work has advanced on the project's heating, ventilation, and air−conditioning system, interior wall stone and ceiling installation, and other interior and exterior construction work. However, some delays have occurred in activities on the project's critical path (i.e., the work on the fire alarm system) and on most of its near−critical paths, and further delays are possible. At the November 15, 2006, CVC hearing, the Government Accountability Office (GAO) reported that the total cost of the entire CVC project at completion is likely to be about $592 million without an allowance for risks and uncertainties, and over $600 million with such an allowance. To date, about $556.2 million has been approved for CVC construction, including about $25.2 million in fiscal year 2007 appropriations. For fiscal year 2007, AOC has also received an additional appropriation of $18.6 million for the CVC project, which AOC has not yet received approval to obligate.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−1149T

[Return to top]

Emergency Services Sector

26. *July 30, Houston Chronicle* — **Texas responders say emergency radios needed for times of disaster.** Law officers and other emergency responders from across Texas met Monday, July 30, to work to ensure their radio communication systems are in sync in case of a terrorist attack or a major natural disaster. Delegates of the Texas Radio Coalition gathered to make recommendations for a unified public safety communications system. The U.S. Department of Homeland Security announced last week that Texas is eligible for a $65 million grant to improve its emergency radio system statewide. Pete Collins, chair of the Texas Radio Coalition,

said local and state officials next will show how they would use the federal money. The goal is not to replace all the local and regional radio systems, but to get updated technology that integrates them, Collins said. Texas Radio Coalition delegates have determined that the Texas−Mexico border region is the state's highest priority because of its location and because there is no communication in some border areas, Collins said.
Source: http://www.chron.com/disp/story.mpl/ap/tx/5011596.html

[Return to top]

Information Technology and Telecommunications Sector

27. *July 31, IDG News Service* — **Mozilla rushes out second Firefox patch this month.** Mozilla has patched a pair of nasty flaws in its Firefox browser, two weeks after security researchers first started posting code that showed how the flaws could be exploited in attacks. The 2.0.0.6 version of Firefox, released Monday, July 30, fixes a pair of related flaws in the URL protocol handler component of Firefox, which is used to launch programs when a user clicks on certain specially crafted Web links. Mozilla rates these problems critical, meaning they are a serious security risk. The 2.0.0.6 Firefox release also fixes a third security flaw, that Mozilla considers to be less−critical than the URL protocol handler bugs.
Mozilla Security Advisory 2007−26:
http://www.mozilla.org/security/announce/2007/mfsa2007−26.ht ml
Mozilla Security Advisory 2007−27:
http://www.mozilla.org/security/announce/2007/mfsa2007−27.ht ml
Source: http://www.infoworld.com/article/07/07/31/Mozilla−second−Fir efox−patch_1.html

28. *July 31, Sophos* — **Hacker exploited unsecured wireless Internet access to send spam.** Sophos has reminded computer users of securing their wireless Internet access following the sentencing of a man who sent pornographic spam while driving around Venice, CA. Nicholas Tombros has been sentenced to three years' probation and six months home detention after e−mailing out thousands of advertisements for pornographic Websites. The spam e−mails were sent from Tombros's laptop via unencrypted wireless Internet access points he found while driving his car.
Source: http://www.sophos.com/pressoffice/news/articles/2007/07/tomb ros.html

29. *July 30, IDG News Service* — **Google Analytics in data blackout since Saturday.** Google Inc.'s Analytics service stopped delivering data to users on Saturday, July 28, another in a series of recent performance and availability problems affecting the popular Website traffic−monitoring service. The latest problem remains unsolved and is apparently affecting all Google Analytics accounts, according to a message posted Monday afternoon by a Google employee in the official Google Analytics blog. Users can log in to their accounts, but the data hasn't been updated since Saturday night. Last week, Google Analytics suffered what the company called a "brief processing delay." Another such delay hit the service during the July 14−15 weekend, affecting "a small percentage of users," Google said at the time. The previous weekend, a server outage prevented "many" users from creating and logging into new accounts, according to Google. A significant data outage left many users fuming in late May as well.
Source: http://www.computerworld.com/action/article.do?command=viewA rticleBasic&articleId=9028462&intsrc=hm_list

Internet Alert Dashboard

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30. *July 31, Monroe News (MI)* — **Mysterious powder dropped in Michigan county.** Law enforcement officials are trying to determine the identity of a substance that was dropped from a low−flying airplane in the Bolles Harbor area in Michigan Monday morning, July 30. Although federal officials have been notified, they do not feel there is a threat. The Monroe County Sheriff's Office reported the plane dropped a white powder substance about 8:22 a.m. EDT. Samples have been collected and were sent to the Michigan State Police crime lab for analysis. The FBI in Detroit and Washington were notified, as well as Homeland Security. Source: http://www.monroenews.com/apps/pbcs.dll/article?AID=/20070731/NEWS01/307310002/−1/NEWS

[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