Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 12 July 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- Authorities have broken up an identity theft and drug ring in three north Georgia counties that had at least 14,000 stolen credit card numbers on a laptop computer; investigators believe much of the financial and identity information was stolen from mailboxes and trash bins by crews of runners. (See item 7)

- For the near term, subway passengers in London are to have their bodies scanned by machines that see through clothing in an attempt to prevent further terrorist attacks. (See item 12)

DHS/IAIP Update *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/IAIP Products &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://esisac.com]

---

1. *July 11, San Francisco Chronicle* — **December tsunami prompts scientists to review all risks to California's nuclear plants.** Six months after the mega−tsunami in the Indian Ocean, fears of a major tsunami on the California coast are spurring scientists to reassess the possible impact on nuclear power plants. PG&E is planning to spend $500,000 in a new effort to assess how two worst−case scenarios for tsunamis –– the "apocalyptic model" and the "decades−of−terror model," as the utility's top geoscientist, Lloyd Cluff, calls them –– would affect the Diablo Canyon nuclear plant near San Luis Obispo, CA, and the decommissioned Humboldt Bay nuclear plant near Eureka, CA. The extreme−worst case, or "apocalyptic model," assumes a magnitude−9 quake involving a simultaneous rupture of the Cascadia

subduction zone and the adjacent Little Salmon Fault in the Pacific Northwest. The "decades of terror model" assumes the possibility of multiple, less extreme quakes that occur over a few decades, each of which might trigger a tsunami. Other institutions assisting PG&E with the study are the U.S. Geological Survey and the Tokyo Earthquake Research Institute in Tokyo.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2005/07/11/ MNG84DLO521.DTL&feed=rss.news

2. *July 11, Reuters* — **General Electric and Canadian firm to buy U.S. gas pipeline system.** General Electric Company (GE) and Canada's biggest institutional investor will buy the Southern Star gas pipeline system from AIG Highstar Capital for $362 million, plus the assumption of $476 million in debt and preferred stock, GE and its partner said on Monday, July 11. The purchase by GE and Canada's Caisse de Depot et Placement du Quebec includes compressor stations and gas storage fields serving local gas distribution companies in Missouri and Kansas, they said. The natural gas pipeline spans 6,000 miles in seven Midwestern and Southern U.S. states. GE said the deal, its second joint investment with the Canadian partner, doubles its pipeline assets. It will hold a 60 percent stake in Southern Star, and its partner will own 40 percent.
Source: http://today.reuters.com/news/newsArticleSearch.aspx?storyID =131866+11−Jul−2005+RTRS&srch=GE+commercial

3. *July 10, San Francisco Chronicle* — **Transbay electric connection $300 million project would send power through buried cables in California.** Electric power is San Francisco's Achilles' heel. The city's aging power plants don't generate the amount of electricity its people need. High−voltage lines tied to the state's power grid take up the slack, but they all come from just one direction−the Peninsula. An earthquake there could shut down several lines at once. Now, the city of Pittsburg, CA and Babcock & Brown, a finance company specializing in power projects, want to bring energy to San Francisco through a new route −− a cable under the bay. They plan a $300 million electrical line running beneath the bay floor from Pittsburg to San Francisco. Buried three to six feet deep for most of its 55 miles, the transbay cable would give the city an extra path for power by providing another route for as much as 400 megawatts from the state grid, or roughly enough to light 300,000 homes. The California Independent System Operator, which runs the state's electrical grid, is expected to vote on the project by the end of this month.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2005/07/10/ BUG8JDLA4V1.DTL&feed=rss.business

4. *July 06, Instrumentation, Systems, and Automation Society* — **New research to fix U.S. power grid.** The federal government is getting engineering researchers involved to develop purely electronic systems in order to make the U.S. power grid more reliable and efficient. Silicon−carbide, solid−state equipment will replace outdated and obsolete electro−mechanical devices such as those that failed to localize the 2003 blackout in the Northeast, the largest and most catastrophic power failure in the history of the country. Silicon−carbide allows an extremely high voltage capability and is a good thermal conductor. Alan Mantooth, University of Arkansas (UA) professor of electrical engineering and director of the newly formed National Center for Reliable Electric Power Transmission, and three other UA electrical engineering researchers received $1 million from the U.S. Department of Energy's GridWorks Initiative to create and operate the new national center. The center's researchers, including faculty and

graduate students, will design, test, and package the electronic systems for future commercial use in the nation's power grid. Funding for new national center is part of the federal government's focus on research and development to improve technology on the nation's power grid. In response to the massive blackout in 2003, Congress passed the Energy Policy Act of 2003 and created the GridWorks Initiative.
Source: http://www.isa.org/Template.cfm?Section=Professionals_and_Pr actitioners&template=/ContentManagement/ContentDisplay.cfm&C ontentID=44856

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *July 11, Washington Post* — **Defense firms consider moving.** In the two months since the Pentagon announced its base closure and reorganization plan, a proposal that would move 23,000 military workers out of Northern Virginia's close–in suburbs, the local government contracting community has been grappling with the potential implications for their businesses. Contractors in the Washington, DC, metropolitan area already are scouting new office space and thinking about moving some of their employees in response to the planned redeployment of tens of thousands of defense personnel throughout the region. But the disruption won't necessarily be all bad. Contractors say the base and office closings recommended by a Pentagon commission could mean more business for them, and give them a chance to lure talented government professionals into the private sector. Though any changes would not be implemented for several years, contractors say they're watching the proposals and efforts to alter the plan closely. What the government contractors will not do, executives say, is forfeit their projects. If the agencies go, the contractors plan to make every effort to follow. The changes could also result in greater opportunities for some local contractors. If the government loses employees who don't want to relocate, their work might be farmed out to private–sector firms.
Source: http://www.washingtonpost.com/wp–dyn/content/article/2005/07 /10/AR2005071000805.html

[Return to top]

Banking and Finance Sector

6. *July 11, Finextra Research* — **London emergency prompted algorithmic shutdown.** The London Stock Exchange (LSE) ordered all market participants to switch off their algorithmic trading systems in an effort to relieve downward pressure on pricing following bomb attacks in central London on Thursday, July 7. The number of equity trades on the LSE reached record levels on Thursday following the bombings, prompting the exchange to contain the situation by declaring a "fast market," in which market makers are relieved of the obligation to offer firm

two−way prices on stocks traded on the electronic order book. As a secondary precaution, the Exchange also instructed all participants to switch off automated trading applications, which are programmed to buy and sell stocks in response to pre−determined price triggers. The Exchange has never ordered the systems to be shut down before. The functioning of London's financial markets after Thursday's bombing is to be investigated by the UK's tripartite financial authorities −− HM Treasury, the Bank of England, and the Financial Services Authority.
Source: http://www.finextra.com/fullstory.asp?id=13955

7. *July 10, Forsyth County News (GA)* — **Large arrest ties identity theft to methamphetamine.** Local authorities in Georgia as well as federal authorities say they have broken up an identity theft and drug ring in three north Georgia counties that had at least 14,000 stolen credit card numbers on a laptop computer. The arrests of 16 people in Forsyth and Lumpkin Counties comes as a result of a drug and check forgery investigation that began in Lumpkin County in mid−June, Lumpkin County Sheriff Mark McClure said Friday, July 8. McClure said victims stretch across the United States. Investigators believe much of the financial and identity information was stolen from mailboxes and trash bins by crews of runners. Authorities also think at least one business' list of customer credit card numbers was obtained, though they don't know where or how. Forsyth Investigator Charlie Adams said many of the credit card numbers were traded by members of the ring in exchange for drugs, mainly methamphetamine. Law enforcement officials said the investigation centered around Louis Garibay, a Forsyth County man suspected of dealing in methamphetamine. Authorities in Lumpkin County also seized methamphetamine valued at $5,000, guns, hundreds of forged checks and a 2002 Chevy truck reported stolen from Forsyth County.
Source: http://www.forsythnews.com/news/stories/20050710/localnews/1 20807.shtml

8. *July 08, InformationWeek* — **Iron Mountain loses more tapes.** City National Bank has become the second company in two months to experience a loss of backup tapes in transit by Iron Mountain Inc. The Los Angeles−based bank disclosed Thursday, July 7, that two tapes containing sensitive data, including Social Security numbers, account numbers, and other customer information, were lost during transport to a secure storage facility. The bank said the data was formatted to make the tapes difficult to read without highly specialized skills, but declines to say if they were encrypted. It said there's no evidence that data on the tapes has been compromised or misused. Iron Mountain said it lost the tapes in April. The tapes were in a small container of backup tapes belonging to a Texas−based Internet services provider that hosts applications for City National and other banks. The incident has been investigated by federal law enforcement officials and no evidence has been found of identity theft relating to the loss. In May, Time Warner revealed that tapes containing data, including names and Social Security numbers, on 600,000 current and former employees disappeared in March while being shipped to an offsite storage facility operated by Iron Mountain.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid= PIVEAQHR4M2RIQSNDBCCKHSCJUMEKJVN?articleID=165701015

[Return to top]

Transportation and Border Security Sector

9.

July 11, Bloomberg — **Amtrak resumes New York–Washington Acela trains.** Amtrak, the national passenger railroad, said its Acela Express high–speed train resumed service with four trips between New York and Washington Monday, July 11, almost three months after being halted because of cracks in a brake part. The trains being run include two services in each direction, Amtrak said in a statement. Before the trains were stopped on April 15, Amtrak ran 15 daily trips between New York and Washington. The railroad didn't say when it would resume New York–Boston Acela service, which was suspended as well.
Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=a5nBabUM 4UII&refer=us#

10. *July 10, Associated Press* — **Report finds high number of runway incidents at Logan.** There were more pilot deviations and control tower errors at Boston, Massachusetts' Logan International Airport than at similarly busy airports in the past year and a half, Federal Aviation Administration (FAA) reports indicate. Pilots had to change their paths to avoid collisions with other planes or airport vehicles eight times between January 2004 to June 1 of this year. Air traffic controllers also made two operational errors during the same 18–month period. The FAA listed all the Logan incidents as having little risk of a collision or as having enough time to avoid a collision. FAA officials told the Boston Globe that Logan's numbers were relatively high. But the agency found an overall reduction of serious runway incidents at Logan and other airports, according to spokesperson Laura Brown. Logan is the nation's 17th busiest airport in terms of total takeoffs and landings. Newark Liberty International Airport, the 15th busiest, and Miami International Airport, the 19th busiest, each had five incidents. New York's LaGuardia Airport, the 19th busiest, had one incident during the same period.
Source: http://www.boston.com/news/local/massachusetts/articles/2005 /07/10/report_finds_high_number_of_runway_incidents_at_logan /

11. *July 09, San Diego Union–Tribune (CA)* — **Train cars left on track.** On Thursday, July 7, a train crew stopped its 44–car freight train in the middle of San Diego, CA, left the engine humming and disappeared. Officers discovered the train around 11 p.m., parked on Morena Boulevard not far from Mission Bay. Police Sgt. Kerry Tom said the crew left a little note behind: "We've worked our maximum allotted hours and we took a taxicab home." Officials for Burlington Northern Sante Fe railroad say such a move –– the crew had worked the federal maximum of 12 hours and had to stop the train –– is neither unusual nor dangerous. In fact, it's typical railroad procedure. The gap between train crews varies, depending on the urgency of the schedule. In this case, it took about one and a half hours for a fresh crew to arrive at the train. There is no federal requirement that crews must stay until they are replaced. A federal Transportation Security Administration official said his office doesn't regard the San Diego incident as cause for alarm. "TSA doesn't see this as a security or a safety breach," said Nico Melendez, the agency's western field director for public affairs. "It is rather standard for locomotive companies to do this. . . . There are steps they take to disable the train."
Source: http://www.signonsandiego.com/news/metro/20050709–9999–1n9tr ain.html

12. *July 08, Times (United Kingdom)* — **Body scan machines to be used on subway passengers.** For the near term, London, England, subway passengers are to have their bodies scanned by machines that see through clothing in an attempt to prevent further terrorist attacks. The wave imagers will be used to carry out random checks as people enter stations. Police and transport officials are also considering installing the equipment permanently at stations across the

network. The technology is already used to catch illegal immigrants who hide in lorries at Channel ports but has not previously been used on the subway because of the high cost and concerns about privacy. The scanners can spot the waistcoat bombs usually worn by suicide bombers and automatically send an alert to nearby officers. Unlike other scanners, they can cover crowded entrances without the need for people to be stopped for individual checks. The system works by measuring the solar radiation reflected by people's bodies and measuring anything which interferes with the reflection. It can be linked to closed−circuit television cameras that will automatically pick out and follow a suspect until he can be stopped and questioned.
Source: http://technology.timesonline.co.uk/article/0%2C%2C20409−168 6151%2C00.html

13. *June 10, Government Accountability Office* — **GAO−05−331: National Airspace System: FAA Has Made Progress but Continues to Face Challenges in Acquiring Major Air Traffic Control Systems (Report).** The Federal Aviation Administration's (FAA) multibillion−dollar effort to modernize the nation's air traffic control (ATC) system has suffered from cost, schedule, and/or performance shortfalls in its system acquisitions for more than two decades. FAA's performance−based Air Traffic Organization (ATO) was created in February 2004, in part, to address these legacy challenges. In this report, GAO examined (1) FAA's experience in meeting cost, schedule, and performance targets for major ATC system acquisitions; (2) steps taken to address legacy problems with the program and additional steps needed; and (3) the potential impact of the constrained federal budget on this program. Secretary of Transportation direct FAA to provide detailed information to Congress about the impact of planned funding cuts on the agency's ability to modernize the ATC system, and the National Airspace System (NAS). In commenting on a draft of this report, the Department of Transportation (DOT), FAA, and ATO said they generally agreed with the report.
Highlights: http://www.gao.gov/highlights/d05331high.pdf
Source: http://www.gao.gov/new.items/d05331.pdf

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *July 11, Agence France Presse* — **Japan region hit by bird flu to cull more chickens.** Japanese authorities said they have discovered the seventh outbreak of bird flu in less than a month in Ibaraki prefecture where some 150,000 chickens have already been been culled. Authorities in Ibaraki, some 60 miles north of Tokyo, said they will start killing 8,550 birds Tuesday, July 12, at the infected farm. The virus has already been discoverd at six other poultry farms in a three−mile radius in Ibaraki, with the first case detected late last month. The strain was of the H5 variety but that tests had yet to identify it further. The first case in Ibaraki was found to be H5N. The Ibaraki government and the agriculture ministry have ordered poultry farms in the area to suspend the transport of chickens and eggs.

Source: http://news.yahoo.com/s/afp/20050711/hl_afp/healthflujapan_0 50711112951

15. *July 11, Houston Chronicle (TX)* — **Ranch shows no more traces of mad cow.** Thirty−eight more cattle from a Texas ranch tested negative for mad cow disease, the U.S. Department of Agriculture (USDA) said Sunday, July 10. The 38 animals were from the same ranch and herd as the Texas beef cow recently confirmed to have mad cow disease. No further testing on those animals is planned. The USDA has screened 67 adult cows from the ranch and herd, all tested negative in rapid screening tests and is through testing animals at the ranch. The USDA is still tracking animals that may be related to or born the same time as the infected cow.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/326049 3

[Return to top]

Food Sector

16. *July 10, Associated Press* — **Wyoming cafe closes amid salmonella reports.** Owners of a Rock Springs, WY, restaurant have voluntarily closed due to a possible link to a salmonella outbreak. Seven or eight cases have been reported in Sweetwater County, and the county Health Department is investigating, the agency's Jodye Wilmes said. The restaurant's owners closed voluntarily and are contacting suppliers to help with the investigation. The food−borne bacterium causes severe nausea, cramps, diarrhea and fever about 12 to 72 hours after contaminated food is eaten. Infections can be life−threatening to the elderly and very young.
Source: http://www.casperstartribune.net/news/wire/ap/?wire_num=2215 18

17. *July 08, Associated Press* — **Cantaloupe items recalled.** OBIM, a producer of fresh−cut fruit, said Friday, July 8, it had issued a recall of various fresh−cut cantaloupe items because of a risk of salmonella contamination. An investigation is under way to determine how the contamination originated and the health risk, OBIM said, though there have so far been no reports of illness stemming from the problem. The products are distributed in Arkansas, Colorado, Kansas, Louisiana, Mississippi, Oklahoma, Alabama, Kentucky, Missouri, Tennessee, and Texas.
Source: http://www.signonsandiego.com/news/state/20050708−2258−canta louperecall.html

[Return to top]

Water Sector

18. *July 11, The Courier−Journal (KY)* — **Water emergency hits parts of Kentucky.** A failed pump has created a water emergency for parts of Shelby County, Frankfort, Georgetown and other locales in Kentucky that get their water from the Frankfort Plant Board water utility. Mandatory water conservation measures are in effect until further notice, when the pump at the utility's water treatment plant is fixed. Because of unusually dry conditions, Shelby County residents were asked to voluntarily conserve water at the end of last month, but the new restriction is mandatory. "This is sort of a panic situation," said Darrell Dees, manager of the North Shelby Water Co. and U.S. 60 water district, which gets its water from the Frankfort supplier. The water emergency also affects these districts Farmdale, Peaks Mill, Elkhorn and

South Anderson.
Source: http://www.courier−journal.com/apps/pbcs.dll/article?AID=/20
050711/NEWS01/507110396/1008/NEWS01

Public Health Sector

19. *July 11, Reuters* — **Bird flu returns to Thailand.** The deadly bird flu virus which has killed 55 Asians has erupted again in Thailand despite a major campaign to eradicate it, the government said on Monday, July 11. Infected fowl were found this month in five places of three districts in Suphanburi province, 60 miles north of Bangkok, during follow−up inspections of previously affected areas, a senior Agriculture Ministry official said. The discoveries reinforced warnings by international health bodies about how difficult it will be to eliminate the H5N1 virus now it has become endemic in parts of Asia. "Infected fowl are living longer due to increasing immunity," Yukol Limlaemthong, head of the ministry's livestock department told Reuters, meaning it was less likely that unusual deaths would alert farmers to the possibility of infection. Twelve Thais have died after being infected by the virus, but there have been no reports of human infections since October in the country. However, 19 people have died in Vietnam since December, when the virus returned, taking the country's toll to 39. Four Cambodians have also died of the disease which first rolled across much of Asia in late 2003.
Source: http://thestar.com.my/news/story.asp?file=/2005/7/11/worldup
dates/2005−07−11T121756Z_01_NOOTR_RTRJONC_0_−208914−1&sec=Wo rldupdates

20. *July 11, Associated Press* — **Blood pressure enzyme may help battle Severe Acute Respiratory Syndrome.** An enzyme that regulates blood pressure also is involved in infection by the Severe Acute Respiratory Syndrome (SARS) virus. Learning how SARS became a deadly threat "possibly teaches us a lesson on how to actively fight diseases such as SARS, avian flu, or the effects of weapons such as anthrax," said Josef Penninger of the Austrian Academy of Sciences. The research may have wider implications for a type of lung failure known as acute respiratory distress syndrome, Penninger reported in a communication to the journal Nature. Researchers report that, working in mice, they found that angiotensin−converting enzyme 2 (ACE2) is a crucial receptor for the SARS virus. The result is disruption of the body's protective renin−angiotensin system, leading to respiratory distress syndrome as fluids seep into the air sacks. The renin−angiotensin system uses enzymes to regulate sodium balance, fluid volume and blood pressure. The researchers found that the SARS virus binds to the ACE2, Penninger said. If disabling ACE2 allowed lung damage to occur, the researchers wondered whether providing more of the enzyme would help. They created more ACE2 and infused it into the mice. The result was to protect mice from the lung failure effects of SARS.
Nature Medicine correspondence:
http://www.nature.com/nm/journal/vaop/ncurrent/abs/nm1267.ht ml
Source: http://www.latimes.com/news/nationworld/politics/wire/sns−ap
−sars−enzyme,1,3109488.story?coll=sns−ap−politics−headlines

21. *July 11, Wall Street Journal* — **U.S. struggles for drugs to counter biological threats.** A $5.6 billion federal program designed to produce new vaccines and drugs to counter biological

threats is struggling, leaving the nation behind in efforts to build a promised defensive stockpile. Big drug and biotechnology companies largely have shunned the program, known as Project BioShield and overseen by the Department of Health and Human Services (HHS), amid concerns over legal liability, high costs, and limited potential for profit. That has left the government highly dependent on fragile, little−known biotech companies −− which all too often are run on a shoestring budget and dependent on government orders simply to stay in business. A year after President Bush signed Project BioShield into law, only one big contract has been awarded −− $878 million for a novel anthrax vaccine. A few smaller contracts have been handed out, but others for promising vaccines and drugs have stalled in the federal health bureaucracy. In 2000, the Defense Science Board, an advisory panel to the Pentagon, identified 57 diagnostics, therapeutics, or vaccines that were needed to respond to a range of diseases or potential biological weapons. Industry experts note that in almost every case, not enough has been produced or made available.
Source: http://www.post−gazette.com/pg/05192/536248.stm

[Return to top]

Government Sector

22. *June 17, Government Accountability Office* — **GAO−05−700: Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program (Letter Report).** The Department of Homeland Security (DHS) relies on a variety of computerized information systems to support its operations. The Government Accountability Office (GAO) was asked to review DHS' information security program. GAO found that DHS has not fully implemented a comprehensive, departmentwide information security program to protect the information and information systems that support its operations and assets. It has developed and documented departmental policies and procedures that could provide a framework for implementing such a program; however, certain departmental components have not yet fully implemented key information security practices and controls. For example, risk assessments—needed to determine what controls are necessary and what level of resources should be expended on them—were incomplete. Elements required for information system security plans—which would provide a full understanding of existing and planned information security requirements—were missing. Testing and evaluation of security controls—which are needed to determine the effectiveness of information security policies and procedures—were incomplete or not performed. Elements required for remedial action plans— which would identify the resources needed to correct or mitigate known information security weaknesses—were missing, as were elements required for continuity of operations plans to restore critical systems in case of unexpected events.
Highlights: http://www.gao.gov/highlights/d05700high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−700

[Return to top]

Emergency Services Sector

23. *July 11, Rome News−Tribune (GA)* — **Drill to test delivery of medicine in emergency.** An

9

interstate homeland security exercise between health officials in Georgia and Tennessee will be held Tuesday and Thursday, July 21. The exercise, one of the first in the nation to test collaboration between two neighboring states, is designed to ensure that large−scale distributions of medication are possible if a public−health problem large enough to deplete local supplies were to emerge. The goal for health workers in participating Floyd County, GA, will be to utilize those national resources to medicate all 95,000 county residents within 72 hours, said Floyd County Health Department Nurse Manager Pat Townley. In order to make the drill a success, the health department needs 500 volunteers to participate, she said. All ages are invited, she added, although those younger than 18 must be accompanied by an adult.
Source: http://news.mywebpal.com/partners/680/public/news645282.html

24. *July 11, Quad−City Times (IL)* — **Emergency response team conducts disaster drill.** The Rock Island, IL, Community Emergency Response Training,(CERT) team, held its first−ever disaster drill Saturday, July 9. And with the use of Rock Island Boy Scout Troop 268 that served as the victims, 40 area people demonstrated their knowledge of what to do in the face of disaster. The Boy Scouts, dressed with wounds, broken arms, and hurt spines, were placed in the building while different teams of CERT volunteers used their knowledge of disaster situations to help. Volunteers practiced getting victims out of the building safely, marking which areas had been searched, lifting a 400−pound concrete slab to rescue a victim trapped underneath and a live fire simulation. Each of the 40 people who participated were required to take 20 hours of classes relating to what to do in emergency situations. While the Red Cross helps organize and put on the disaster relief classes and drills, grants from the national Homeland Security office offset the approximately $200 per−person cost to provide instructor fees and a backpack filled with supplies.
Source: http://www.qctimes.net/articles/2005/07/10/news/local/doc42d 09a26f2905410992465.txt

25. *July 11, Associated Press* — **Graniteville train wreck DVD now a training tool.** Shortly after the Graniteville, SC, train wreck involving hazardous materials in January, Lt. Ed Schuler of the Aiken County Hazmat team began compiling audio and video clips to give a glimpse of what it was like to see the destruction firsthand. The result, a dramatic 20−minute vide has been shown to emergency workers at conferences around the country as a reminder of the dangers of hazardous material incidents. The video's message: Don't rush in to an incident when you're not exactly sure what's going on. That was a lesson learned from the Sept. 11, 2001, attacks on the World Trade Center when police officers and firefighters ran into the buildings only to be killed when the towers collapsed. In Graniteville, many residents were awakened by the early morning wreck and third−shift mill workers frantically called 911 complaining of breathing problems and itchy eyes. The emergency response to the disaster has been praised by local, state and federal agencies. But Schuler hopes more can be learned from the incident, especially using the documentary's emotional impact.
Source: http://www.thetandd.com/articles/2005/07/11/news/doc42d1f732 e3687730334400.txt

26. *July 10, The Journal News (NY)* — **Responders practice river evacuation.** The Westchester Office of Emergency Management, the Rockland Office of Fire and Emergency Services and the U.S. Coast Guard Auxiliary organized a drill focused on evacuation and search and rescue, as well as agency coordination, on Saturday, July 9. The drill was designed to prepare the response if a boat or ship becomes disabled in the event of fire, an explosion or technical

problems. Volunteers from police, fire and medical services from throughout Westchester, Rockland and New York City in New York rode alongside the ferry in rescue boats to evacuate volunteer victims. They also pulled bodies––dummies were used––from the river using a special netting for water rescues. Divers searched the murky Hudson waters for bodies and combed the bottom of the boat where, in an emergency, they might have to search for people or for explosive devices.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/200 50710/NEWS02/507100310/1018/NEWS02

27. *July 10, Morning Sun (MI)* — **Rescuers gain new skills for handling airplane crashes.** A training exercise that simulated an aircraft filled with victims had crashed took place at Mt. Pleasant Airport in Michigan on Saturday, July 9. Around 60 Isabella County fire personnel spent hours in the hot sun dressed in protective gear experiencing what might happen if a burning aircraft landed at the municipal airport only two miles from a heavily populated area. Capt. Michael Smith said the environmentally approved propane fuel used in place of jet fuel throws off an intense heat that makes climbing inside the aircraft just as difficult. "We had to work our way to the cockpit to shut down the throttles," he said. Mt. Pleasant Fire Department and Isabella County Emergency Management hosted the unique drill using a 50–foot aircraft mobile training simulator owned by the state of Michigan and operated by Kellogg Community College in Battle Creek. Program Coordinator Joe Teixeira said the simulator was built in Canada in 1995. Since Sept. 11, the simulated scenario includes training for a terrorist act. One scenario Saturday included a terrorist who had detonated a bomb on an aircraft that crashed at the airport.
Source: http://www.themorningsun.com/stories/071005/loc_train001.sht ml

[Return to top]

Information Technology and Telecommunications Sector

28. *July 11, Houston Chronicle (TX)* — **Texas utility to offer broadband over power lines.** CenterPoint Energy is testing a system to bring high–speed Internet access to consumers through the electric wall socket. The company that owns the power lines throughout Houston, TX, is running a pilot of the system in a residential neighborhood, offering Internet access at speeds more than one–and–a–half times the speed of services offered through cable modems. The technology, called broadband over power lines, or BPL, has long been used by power companies to monitor and manage their electric grids, said Thomas Standish, chief operating officer of CenterPoint's Electric and Information Technology business. With a BPL system, electric retail providers could potentially turn on the service themselves in a matter of minutes, he said. BPL works by sending data via radio waves over power lines. The signal can then either be turned into a wireless data signal and beamed from the power pole outside a customer's home to a wireless modem inside the home, or continue into the house to a modem that plugs into an electrical outlet.
Source: http://www.chron.com/cs/CDA/printstory.mpl/tech/news/3259278

29. *July 11, Reuters* — **Cell phone service disabled in New York tunnels after London attack.** Cellular phone service has been shut off in four busy New York commuter tunnels since last week's deadly blasts in London, officials said Monday, July 11. No specific reason was given

for the move, but cell phones have been used to trigger bombs in the past. Cell phone service is disabled in the Holland and Lincoln tunnels that connect Manhattan to New Jersey under the Hudson River, the Midtown Tunnel to the city's Queens borough and the Battery Tunnel to Brooklyn, officials said. The move came immediately after the bombings in London on Thursday, according to a spokesperson for the Port Authority of New York and New Jersey, which oversees operation of the Lincoln and Holland tunnels. In March 2004, bombs in Madrid that killed 191 people on trains were fitted to mobile phones, using the alarms as timers. Police in London have said they believe the subway bombs there were detonated by timers. A spokesperson for the New York Police Department said officials would weigh the benefits of disabled service against allowing cell phone service in the tunnels so the public could report suspicious packages or individuals.
Source: http://www.computerworld.com/mobiletopics/mobile/story/0,108 01,103125,00.html

30. *July 11, TechWeb News* — **Sprint to acquire U.S. Unwired for $1.3 billion.** Sprint announced Monday, July 11, that it plans to acquire its mobile phone affiliate, US Unwired, for $1.3 billion. In addition to expanding Sprint's direct mobile service by some 500,000 subscribers, the acquisition will halt US Unwired's attempt to block Sprint's merger with Nextel Communications. The deal covers a sweeping subscriber area covering nine states and some 8 million people. The US Unwired units involved in the acquisition are Gulf Coast Wireless, Georgia PCS, and Louisiana and Texas Unwired. US Unwired's coverage includes portions of Alabama, Arkansas, Florida, Georgia, Louisiana, Mississippi, Oklahoma, Tennessee, and Texas. US Unwired employs some 600 persons and had $408 million in revenues in 2004.
Source: http://www.informationweek.com/story/showArticle.jhtml;jsess ionid=S0HHA0YAALVXQQSNDBCSKHSCJUMEKJVN?articleID=165701260

31. *July 11, Federal Communications Commission* — **FCC consents to ALLTEL Corporation acquisition of Western Wireless Corporation licenses and authorizations.** The Federal Communications Commission (FCC) on Monday, July 11, consented to the applications filed in connection with the proposed merger of ALLTEL Corporation and Western Wireless Corporation (WWC) subject to certain conditions. The transactions would transfer the control of licenses held by WWC and its subsidiaries to Widgeon Acquisition LLC, a wholly−owned subsidiary of ALLTEL. The Commission denied all of the petitions filed in opposition to the merger, finding that the merger as conditioned would serve the public interest.
Source: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC−259932 A1.pdf

32. *July 11, internetnews.com* — **US−CERT warns of latest trojan horse attacks.** The US−CERT issued an alert last week warning of heightened trojan virus attacks against companies and individuals. Although trojan attacks that infiltrate computer systems aren't new, US−CERT said the technique used in these latest attacks have two distinct elements, which pose a threat to computing infrastructure and individual business operations. First, the trojans can elude conventional protective anti−virus software and firewalls. A number of open source and tailored trojans, altered to avoid anti−virus detection, have been used. Second, the e−mails are sent to specific or targeted recipients. Unlike "phishing" attacks, the e−mails use subject lines often referring to work or other subjects that the recipient would find relevant. US−CERT made 12 recommendations for system administrators in order to head off trojan horse attacks. They include using an anti−virus scanner on all e−mail attachments, updating operating system and application software to patch vulnerabilities exploited in the past by these Trojans; and turn

off 'Preview Pane' functionality in e−mail clients and set the default options to view opened e−mails as plain text.
Technical Cyber Security Alert TA05−189A −−Targeted Trojan Email Attacks:
http://www.us−cert.gov/cas/techalerts/TA05−189A.html
Source: http://www.esecurityplanet.com/alerts/article.php/3519236

33. *July 10, The Register* — **UK police request pictures, e−mail, phone records in bomber hunt.** London police have asked the public to turn in pictures from mobile phones and video pictures as they hunt the terrorists behind the bomb attacks on the UK capital Thursday, July 7. The call came as Britain's authorities sought to secure email and mobile phone records as they continue their hunt for the bombers. Much of the media networks' coverage of the bombings came from stills and video captured on camera phones and other mobile devices. London's Metropolitan Police on Sunday asked people who captured images on Thursday, both before and after the bombings, and either in or close to the areas where the bombings happened, to forward them to images@met.police.uk. "These images may contain crucial information which could help detectives in what is a painstaking and complex inquiry," said the head of the Met's Anti−Terrorist Branch, Deputy Assistant Commissioner Peter Clarke.
Source: http://www.theregister.co.uk/2005/07/10/london_bomb_sunday/

34. *July 08, TechWeb News* — **Linux compression format flaw found.** A critical flaw in a compression format widely used in Linux and Unix can give hackers a way into machines, security experts said Friday, July 8. A patch for the zlib library isn't available, but several Linux and BSD distributors have rolled out fixes of their own. The bug, which affects the current version of zlib, 1.2.2, can be exploited to create a denial−of−service (DoS) attack, which could crash any application using the library or let the attacker plant code of his own remotely, according to an alert by Danish security firm Secunia. The company rated the zlib vulnerability as "Highly critical," its second−most dire ranking.
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=165701026

Internet Alert Dashboard

be found in the following US−CERT Vulnerability Note: VU#442845 − Multiple PHP XML−RPC implementations vulnerable to code injection US−CERT encourages administrators to apply the appropriate updates, patches, or fixes as soon as possible. If upgrading is not feasible or convenient at this time, then administrators should consider disabling the affected XML−RPC libraries.

Current Port Attacks

Top 10 Target Ports	1026 (−−−), 6881 (bittorrent), 445 (microsoft−ds), 139 (netbios−ssn), 27015 (halflife), 80 (www), 135 (epmap), 53 (domain), 32775 (sometimes−rpc13), 4672 (eMule)
	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

35. *July 11, WJZ 13 (MD)* — **Efforts underway to boost mall security bill.** New efforts are happening to keep malls and shopping centers safe in Baltimore County, MD. Maryland lawmakers passed a new law requiring that surveillance cameras be installed in the parking lots of large shopping centers. Now a panel studying security at Baltimore County malls wants the law expanded to industrial areas and large commercial spaces.
Source: http://wjz.com/localstories/local_story_192112858.html

[Return to top]

General Sector

36. *July 11, Associated Press* — **Wildfire threatens 750 buildings in Colorado.** A fast−moving wildfire had engulfed 8,000 acres by Monday, July 11, threatening 750 houses, outbuildings and other structures in Beulah, CO, and the surrounding ranching community 150 miles south of Denver. About 5,000 people have been evacuated in Pueblo and Custer counties in southern Colorado since the lightning−sparked blaze was discovered Wednesday, July 6, said Rocky Mountain Area Coordination Center spokesperson Jen Chase. The blaze was burning largely out of control Monday, July 11, with crews able to contain five percent of it. Governor Bill Owens declared a state of emergency for the area and authorized the use of state emergency funds to help with fire fighting expenses.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/11/AR2005071100234.html

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

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.

DHS/IAIP Disclaimer

The DHS/IAIP 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.