Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 13 July 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The California Independent Systems Operator says that Southern California faces potential blackouts if unusually high temperatures persist this summer. (See item 1)

- Wired News reports law enforcement officials, concerned that terrorists will exploit emerging in−flight broadband services to remotely activate bombs or coordinate hijackings, are asking regulators for the power to begin eavesdropping on any passenger's Internet use. (See item 11)

- The US−CERT has released Technical Cyber Security Alert TA05−193A: Microsoft Windows, Internet Explorer, and Word Vulnerabilities. (See item 30)

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 12, Silicon Valley/San Jose Business Journal (CA)* — **High temperatures trigger power grid warning in California.** The California Independent Systems Operator (ISO) warned power plant operators throughout California not to do any unnecessary maintenance operations between 8 a.m. and 10 p.m., July 12, due to high temperature forecasts throughout California. "Market participants are cautioned to avoid actions, which may unnecessarily jeopardize generator availability," an ISO spokesperson said. Southern California faces potential blackouts

if unusually high temperatures persist this summer, according to ISO estimates. Northern California should have adequate supplies this summer as long as power plants expected to be operating do not go off line.
Source: http://www.bizjournals.com/sanjose/stories/2005/07/11/daily1 4.html?from_rss=1

2. *July 11, Market Watch* — **Federal Energy Regulatory Commission head looks to overhaul policies.** As chairman of the Federal Energy Regulatory Commission (FERC), Joseph Kelliher announced Monday, July 11, he will seek to overhaul long−standing power transmission, natural gas storage, and generation policies over the next two years of his term. Kelliher's agenda includes securing congressional authority to approve deals limited to transferring ownership of power plants, a review process that currently rests with antitrust agencies that typically do not intervene unless there is evidence of a monopoly. Kelliher also said he plans to look at some of the policies governing the operation and use of the 150,000 miles of high−voltage transmission lines that make up the nation's power grid. The chairman wants to reform the so−called open access transmission tariff for investor−owned utilities that control transmission. The tariff was created in the mid−1990s as part of the move to open wholesale electric power sales to competition. Regulators are concerned, however, that companies owning transmission lines can use the tariff to discriminate among users and thwart competition. In addition, Kelliher plans to review the costs being generated by some of the independent regional transmission organizations that control large parts of the grid, as well as tackling outdated natural gas storage pricing policies.
Source: http://www.marketwatch.com/news/story.asp?guid=%7B68B53DF0%2D96F6%2D4A64%2D989D%2D5336A05E11B5%7D&dist=rss&siteid=mktw

3. *July 10, Portland Press Herald* — **Approval of gas terminal in Maine by Bureau of Indian Affairs.** The Bureau of Indian Affairs has approved an agreement between Quoddy Bay LLC and the Passamaquoddy Tribe to build a Liquefied Natural Gas (LNG) terminal in the far−eastern corner of Maine. The approval is just the first of many required, but the developers are hopeful that they can have such a facility operational by 2009. The siting of an LNG facility on the Maine coast has been controversial. From an industry point of view, the state is well−suited as a site for the terminal because of the natural gas pipeline that runs the length of the Maine coast down to Boston. Until the Passamaquoddy Tribe gave its approval for development of a terminal on its land, however, no local community was willing to host such a facility. Among impacts associated with the terminal are questions about its environmental impact and security. However, the construction jobs associated with building the facility would bring 80 full−time jobs paying an average of $75,000 a year. It would also provide the tribe with a steady source of income, ranging from $6 million to $16 million annually.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpp%5EZmuvpntuXTfc%7DGJ%7Bbfek%5Cv

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

4. *July 12, Aviation Now* — **Capabilities approach changing industrial base, study says.** The U.S. industrial base is "well positioned" to develop and apply the 1,428 most critical war−fighting technologies that the Department of Defense (DoD) seeks, with U.S. suppliers trailing foreign firms in only 7% of the technological areas, a DoD policy study has concluded. The conclusion stems from the final Defense Industrial Base Capabilities Study (DIBCS), this one on focused logistics, published June 30 by the Office of the Deputy Under Secretary of Defense for Industrial Policy. One conclusion drawn from this report is Pentagon leadership has now reorganized around new functional concepts of jointness and capabilities−based warfighting, resulting in large changes to the defense industrial landscape. To that effect, 64% of the total technologies are either new ways of doing business or breakthrough technologies. Furthermore, according to the final study, U.S. suppliers have no foreign competition for nearly 20% of the technologies. Overall, the U.S. base leads in 55% of researched technologies, and is even with the foreign base in 38%. In particular, U.S. industry has the greatest lead in technologies making up battlespace awareness and force application, owning 70% leadership in each sector.
   Defense Industrial Base Capabilities Study: Focused Logistics:
   http://www.acq.osd.mil/ip/docs/dibcs_fl_6−30−05.pdf
   Source: http://aviationnow.ecnext.com/free−scripts/comsite2.pl?page=aw_document&article=INDB07125

[Return to top]

Banking and Finance Sector

5. *July 12, Reuters* — **TD Banknorth to buy Hudson United Bancorp.** TD Banknorth Inc. on Tuesday, July 12, said it agreed to buy New Jersey−based Hudson United Bancorp Inc. for $1.9 billion to expand in the affluent U.S. Northeast. The acquisition is Portland, ME−based TD Banknorth's first major purchase since Canada's Toronto−Dominion Bank paid more than $3 billion for a 51 percent stake in the company four months ago. It will enable TD Banknorth to add 204 branches in New Jersey, Pennsylvania, Connecticut and New York. The purchase also extends the recent consolidation among several Northeast U.S. banks, which analysts expect to continue. “Banknorth has been given a mandate by Toronto−Dominion to expand through acquisition,” said Gerard Cassidy, an analyst at RBC Capital Markets in Portland. “Hudson United has been for sale for about three years. Banknorth has historically been unable to buy it, but its new parent gave it the ammunition,” said Cassidy. The purchase is expected to close in the first quarter of 2006, pending shareholder and regulatory approval. Several non−U.S. banks have eyed the United States for growth, including Royal Bank of Canada and Bank of Montreal, which owns Chicago's Harris Bank, as well as Britain's HSBC Holdings Plc and Royal Bank of Scotland Plc.
   Source: http://www.nytimes.com/reuters/business/business−financial−h udsonunited.html

6. *July 12, Associated Press* — **Australia, Philippines to sign intelligence pact to fight money laundering, terrorism.** Australia and the Philippines have agreed to exchange financial intelligence to help fight money laundering and prevent terrorists from moving money around

the world, Australian Justice Minister Chris Ellison said Tuesday, July 12. The Philippine financial intelligence unit was last week admitted to the Egmont Group, a body of 84 financial intelligence organizations worldwide. "The signing of this memorandum of understanding will now enable the formal exchange of vital financial intelligence between Australia and the Philippines, strengthening the war on money laundering and terrorism financing in this region," Ellison said. Australia has signed similar agreements with 41 other countries across Southeast Asia, the Pacific, South America, Europe and north America, making it harder for terrorist groups and their backers to move illegal funds around the world undetected.
Egmont Group: http://www.egmontgroup.org/
Source: http://asia.news.yahoo.com/050712/ap/d8b9n3u80.html

7. *July 12, Reuters* — **European Union moves to curb terror funding.** The European Union (EU) has agreed to speed up measures to cut off funding for terrorist groups after bombs killed at least 52 people in London last week. British Chancellor of the Exchequer Gordon Brown said after chairing a meeting of EU finance ministers the 25−nation bloc was united in its desire to destroy the monetary lifelines used by groups accused of terrorism. The EU had already adopted an action plan to combat money laundering and banking secrecy that help the illegal moving of money following the September 11 attacks on the U.S. and the March 2004 Madrid bomb blasts. "Banks can no longer operate on the principle that they can provide services to anybody," Brown said. Treasury officials said no new initiatives were planned during Britain's six months in the EU chair, but greater energy would be put into implementing existing measures such as blacklisting suspects, seizing their assets, and exchanging data between financial authorities. Brown said cutting off financing for groups perpetrating attacks was a crucial preventative measure. However, he said he was concerned that some countries outside the EU and America were not doing enough to combat money laundering.
Source: http://edition.cnn.com/2005/WORLD/europe/07/12/terror.funds. reut/

[Return to top]

Transportation and Border Security Sector

8. *July 12, Department of Transportation* — **Funds for Lower Manhattan recovery projects.** The Bush Administration on Tuesday, July 12, awarded nearly a billion dollars to the states of New York and New Jersey to be used for transit projects in and around the World Trade Center site. The $899 million total marks the second installment to help pay for work to rebuild the transit system destroyed by the September 11, 2001 attacks in Lower Manhattan. The Port Authority of New York and New Jersey received $478 million to construct a security center for the southern World Trade Center site. The security center will screen all vehicles for security threats and will be a vital component to the World Trade Center Master Plan. A second grant for $221 million has also awarded for the Port Authority Trans−Hudson (PATH) terminal. To date, the Federal Transit Administration has awarded over $3.86 billion for Lower Manhattan recovery projects out of the $4.55 billion appropriated by Congress. That amount includes $2.95 billion, awarded for initial projects identified by the State of New York. Those projects included the permanent PATH terminal, Fulton Street Transit Center, South Ferry terminal station, as well as first phase of the Route 9A/West Street project.
Source: http://www.dot.gov/affairs/fta1805.htm

9. *July 12, Associated Press* — **Dogs, people still best 'gadgets' in securing mass transit.** Within hours of the London bombings, a renewed call went up for the United States to use its considerable technological heft to prevent similar attacks on the nation's transit system. Public transit's chief lobbyist said its members need $6 billion to upgrade security, and Congress is expected to increase funding in the coming weeks. Sensing opportunity, some technology companies aggressively advertised their potential to create gadgets to detect bombs and chemical and biological weapons. But ideas such as smoke−detector−like devices sounding an alarm when a bomb−porting terrorist enters a train station are years and billions of dollars from fruition. The best current defenses for the country's subways, buses and trains, security experts say, remain decidedly low tech: human vigilance and bomb−sniffing dogs. The very nature of mass transportation makes it impossible to install metal detectors and take the other security measures that aim to protect the flying public. BBN Technologies of Cambridge, MA, believes that while technology might help police collar a terrorist mastermind and thus prevent subsequent attacks, asking tech to prevent bombings is an enormously tall order.
Source: http://www.signonsandiego.com/news/nation/terror/20050712−0010−bomb−sniffingtech.html

10. *July 12, Reuters* — **Cell phone service resumed in two tunnels.** Cell phone service resumed in two of four busy New York commuter tunnels late on Monday, July 11, after it was shut off amid heightened security concerns following last week's deadly blasts in London, officials said. No specific reason had been given for the move to stop service on Thursday, July 7, after the London blasts, which killed more than 50 people, but cell phones have been used to trigger bombs in the past. A New York Police Department spokesperson said police had not requested the shutdown of service in the Midtown Tunnel, which connects Manhattan and the borough of Queens, and the Battery Tunnel between Manhattan and Brooklyn. In announcing the resumption of service, the Metropolitan Transportation Authority (MTA) said, "It appears to be a miscommunication between the NYPD and the MTA." Cell phone service in the Holland and Lincoln tunnels, which go under the Hudson River to connect Manhattan and New Jersey, remained suspended on Monday. The Port Authority of New York and New Jersey, which oversees the Lincoln and Holland tunnels, said it did not consult police before deciding to shut down service in the interest of safety last week.
Source: http://today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2005−07−12T164615Z_01_N11515557_RTRIDST_0_TECH−SECURITY−CELLPHONES−DC.XML

11. *July 11, Wired News* — **Officials fear airplane broadband terror.** Federal law enforcement officials, fearful that terrorists will exploit emerging in−flight broadband services to remotely activate bombs or coordinate hijackings, are asking regulators for the power to begin eavesdropping on any passenger's Internet use within 10 minutes of obtaining court authorization. In joint comments filed with the Federal Communications Commission (FCC) on Tuesday, July 5, the Justice Department, the FBI, and the Department of Homeland Security warned that a terrorist could use on−board Internet access to communicate with confederates on other planes, on the ground or in different sections of the same plane. The Communications Assistance for Law Enforcement Act was originally passed to preserve the Bureau's ability to eavesdrop on telephone calls in the digital age. But last year the FBI and Justice Department persuaded the FCC to interpret the law so it would apply to Internet traffic over cable modems and DSL lines. The FCC has already expressed the view that in−flight broadband would likely

be covered as well. Officials also expressed concern that terrorists might use in−flight broadband to remotely trigger a bomb hidden on a plane. They asked the FCC to keep such services from being accessible from the cargo hull of an aircraft.
Source: http://www.wired.com/news/technology/0,1282,68147,00.html?tw =wn_tophead_1

12. *July 10, Star−Ledger (NJ)* — **Escaping from trains under river now easier.** For train riders, it's a nightmare scenario: a terrorist attack or accident that traps them in a tunnel under the river. Now, after three years of painstaking underground work, a nearly half−billion−dollar project aimed at making the two−mile ride through New York’s Hudson and East River tunnels safer in an emergency is substantially complete, transit officials say. The changes, financed with federal funds in the wake of the September 11, 2001, terrorist attacks, are meant to provide better evacuation, ventilation, firefighting and communications during a tunnel catastrophe. Train riders on Amtrak, NJ Transit, and the Long Island Rail Road will be able to walk shorter distances to safety during evacuation while breathing cleaner air, according to transit officials. The improvements hold renewed importance for the region's travelers following the Thursday bombings in London's subway system, which killed dozens and briefly shut down the city's transit system. The long−awaited improvements −− funded in part by a $100 million grant from the Federal Railway Administration, with the rest coming from the three transit agencies −− addressed emergency response deficiencies in the tunnels that have been cited in reports by both the Department of Transportation and the New York state Legislature.
Source: http://www.nj.com/news/ledger/index.ssf?/base/news−1/1120971 74643380.xml&coll=1

13. *July 08, Hudson Valley News story (NY)* — **Coast Guard increases vigilance, presence following London bombings.** The U.S. Coast Guard −− along with federal, state, and local law enforcement agencies −− has increased its presence aboard passenger ferries and added additional vessel and helicopter patrols around the Port of New York and New Jersey following the early morning bombings in London. Also, Coast Guard vessels have been stationed in the Hudson River in the vicinity of the Indian Point nuclear power plants in the past during heightened states of alert after the September 11th attacks. Witnesses who observe suspicious activity along our nation's waterways are encouraged to contact the nearest Coast Guard command, the Coast Guard's America's Waterway Watch hotline at 877−24−WATCH, or the National Response Center hotline at 1−800−424−8802.
Source: http://www.midhudsonnews.com/News/London_reax_CG−08Jul05.htm

[Return to top]

Postal and Shipping Sector

14. *July 12, Tallahassee Democrat (FL)* — **Dennis shuts down St. Marks post office.** The U.S. Postal Service is working to make sure the people in Pensacola and Wakulla, FL, affected by Hurricane Dennis get their mail. But the St. Marks Post Office will not be up and running anytime soon. Joseph Breckenridge, a postal service spokesperson, said it will take four months to repair the building. "We aren't going to close the post office in St. Marks," Breckenridge said. "It's just going to take us a while to get it up and running." Farther west in the Panhandle, many post offices are without power, Breckenridge said. Generators, fans, and lights will be moved into the still−operable offices and service will continue. The main post office is still

open in Pensacola, but the surrounding offices have limited retail. Because of the lack of power and the large number of employees that left the state to escape Dennis, carriers are delivering only 35 percent of the mail. Breckenridge said home delivery Tuesday, July 12, is expected to increase to 60 percent and be up to 100 percent in most places by Thursday, July 14.
Source: http://www.tallahassee.com/mld/tallahassee/news/local/121102 15.htm

15. *July 12, Associated Press* — **Congressional correspondence mostly e−mail.** Nine out of 10 letters sent to the U.S. Congress are sent vie e−mail, according to a report that chronicles the rapid shift from postal letters to e−mail as the means of communicating with lawmakers. The report, based on a survey of 202 House and Senate offices, found that Congress received 200 million e−mail and postal mail messages in 2004, four times the 50 million total in 1995. During that period, postal mail dropped sharply, from 50 million a decade ago to about 18 million last year. The convenience of e−mail has become even more marked since the discovery of anthrax in letters sent to the Capitol shortly after the September 11 attacks. However, the report found that the benefits of speedy e−mail often work only in one direction. Lawmakers generally have not increased the number of personnel to handle the jump in communications, and many still reply through postal mail. Only 17 percent of House offices and 38 percent of Senate offices answer all their e−mail messages with e−mail, the survey found.
Source: http://washingtontimes.com/national/20050711−104818−5000r.ht m

[Return to top]

Agriculture Sector

16. *July 12, Associated Press* — **Chronic wasting disease experts gather for symposium.** Chronic wasting disease (CWD) has been in the U.S. deer herd for at least 30 years. Questions about why it got there and how it spreads have been around for just as long. Experts on the disease gather in Madison, WI, this week to share their research on the disease. The symposium of researchers, academics, and wildlife officials will give them a chance to swap information and strategies on a disease that has spread beyond the Colorado areas where it was first discovered. State and federal officials organized their first symposium on the subject in Madison three years ago, not long after it popped up in the state deer herd. This year's three−day event features a series of panel discussions on such topics as how the disease is spread and how some states have tried to contain it within their deer populations.
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/local/ 12111033.htm

17. *July 12, Associated Press* — **Hurricane Dennis' remnants may spread soybean rust.** Remnants of Hurricane Dennis could bring more than rainfall to the Midwest's parched fields: The storm clouds also could carry spores of a potentially devastating soybean fungus. When Dennis made landfall along the Gulf Coast Sunday, July 10, it swept an area of southwestern Alabama where fields are infected with soybean rust, said Purdue University plant pathologist Greg Shaner. The storm then moved into the Tennessee and lower Ohio valleys, and on Tuesday, July 12, rain was falling across Missouri and Illinois. Shaner said farmers and agricultural scientists nationwide will be looking for any signs over the next few weeks that the fungus has spread. "The message we're trying to get out is that farmers should be out scouting their fields for this fungus. The more people we have out looking the better," Shaner said. Soybean rust has not caused any significant damage in the U.S. since it arrived in 2004 from

South America −− likely on the winds of Hurricane Ivan. The fungus was confirmed in eight states last year, but so far this year, active infections have been confirmed only in Alabama, Florida, and Georgia.
Source: http://www.nytimes.com/aponline/business/AP−Farm−Scene.html? oref=login

18. *July 12, Associated Press* — **Horse disease found in Pennsylvania.** A horse sold at an auction tested positive for a deadly disease and state agricultural officials are trying to prevent the disease from spreading. The horse, sold at the Meadville, PA, Livestock Auction on June 29 tested positive for equine infectious anemia. The horse left an Ohio sale with EIA test results pending. Pennsylvania regulations forbid the importation of horses that have not been tested and shown to be negative for EIA, said Bruce Schmucker, a veterinarian with the state Department of Agriculture's Bureau of Animal Health. The agriculture department issued an alert to area veterinarians and horse farmers suggesting that any horse purchased from the auction on June 29 be tested for the disease. Equine infectious anemia is often fatal within two to three weeks of the appearance of initial symptoms, according to the U.S. Department of Agriculture. Horses that survive an initial acute stage of the disease are sometimes left with chronic debilitating illnesses that can become acute at any time. Some horses never show symptoms, but once infected they always remain carriers, Schmucker said. It is transmitted primarily by biting flies, he said.
Source: http://www.philly.com/mld/philly/news/12110590.htm

19. *July 11, Ontario Soybean Growers (Canada)* — **Ontario Soybean Rust Coalition launches new Website.** A new Website sponsored by the Ontario Soybean Rust Coalition (OSRC) provides weekly updates on the spread of Asian Soybean Rust in the Southern U.S. and scouting information for Ontario, Canada. The Webpage provides valuable maps of Ontario with information about soybean growth stages, rust treatment recommendations for Ontario growers, and scouting information by county. “Ontario is part of an extensive North American network of crop scientists all working to monitor, forecast, and control the spread of this disease,” says Albert Tenuta, Field Crop Plant Pathologist. “Early detection of Rust is key to minimizing its spread and its effect on yields, and this Website will help get information out quickly and effectively.” The maps posted on the Website use GPS technology. Crop scouts frequently check the growth stage and health of plants at dozens of sentinel plots across the province and upload their findings.
Website: http://soybean.on.ca/rustinfo.php
Source: http://soybean.on.ca/newsarchive_view.php?id=145

20. *July 11, Associated Press* — **Quarantine lifted after ranch cleared of mad cow.** After negative tests on 67 of its animals, the ranch that produced the first native case of mad cow disease in the U.S. had a quarantine lifted Monday, July 11, by Texas animal health officials. The negative results for the brain−wasting disease came back on animals tested from the herd because of their age proximity to the 12−year−old diseased cow. Those destroyed for testing were born the year before, the year of, and the year after the infected animal's birth. The lifting of the hold order, which went into effect June 10 when U.S. Department of Agriculture (USDA) Secretary Mike Johanns announced he was sending samples to England for further testing, will allow animals to come and go from the ranch. Since June 2004, six months after a Canadian−born Holstein shipped to Washington state became the first U.S. case of the disease, the USDA has tested more than 400,000 cows. Initial screening on the Texas cow indicated the

presence of the disease, but results from more sophisticated tests were negative, and the department declared the animal to be free of mad cow disease. The USDA's internal watchdog ordered another round of tests last month that came back positive, and a laboratory in England confirmed the results June 24.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/326049 3.html

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

21. *July 11, ABC7Chicago.com* — **Drought puts stress on water wells across Chicago.** The extreme drought in the Chicago, IL, area is not only affecting farms, gardens and lawns, but the water table for the area as well. Many wells are reaching extremely low levels. This drought is one of the worse in northern Illinois with a deficit of 8.68 inches. According to Paul Young of North Aurora Water Operations, the deep well system has been the most serious aspect affected. “We’ve experienced about 100 to 120 feet of dry out in that table," said Young. Because of the low water levels, all watering is now banned in north Aurora. Since the ban went into effect about a week−and−a−half ago, the demand on the north Aurora aquifer has decreased substantially. This has allowed a nice recovery in the water levels. "We're showing improvement. There is less water demand on our system. And that we're increasing the aquifer itself," said Young. North Aurora isn't the only community feeling the effects of the drought. "Oswego is in a water ban, Batavia, Geneva. We're on the same system, everybody is experiencing a problem," said Young.
Source: http://abclocal.go.com/wls/news/071105_ns_drought.html

[Return to top]

Public Health Sector

22. *July 12, Denver Post (CO)* — **Anthrax test prolonged scare.** The emergency response to the Fort Collins, CO, anthrax scare in June 2005 was generally good, though there was one glaring exception −− it took too long to determine there was no anthrax threat. That's the conclusion of Risk Management Alliance, a firm hired by the Poudre Fire Authority to review and improve the handling of emergency situations. The company examined the sequence of events June 6 when an employee in the Larimer County Department of Motor Vehicles noticed a rash on her arms and a white powder−like substance on the blazer she was wearing. "Everybody felt like the time it took to determine there was no anthrax took probably five and half hours," said Jason Mantas, spokesperson for the Fire Authority. "Nobody feels it needs to take five and a half hours." The primary problem last month was getting conclusive test results, the report said. Both the state health department and Colorado State University's (CSU) Veterinary Diagnostic Laboratory can test for anthrax. But CSU's lab is authorized to test only "noncredible threat

substances," and because two field tests indicated the material was anthrax, the lab needed a go−ahead from law enforcement to conduct the test, the report said.
Source: http://www.denverpost.com/news/ci_2853132

23. *July 12, Associated Press* — **Second polio case found in Angola.** A second case of polio has been diagnosed in Angola, suggesting that the disease could be spreading in the southwest African country, the World Health Organization (WHO) said Tuesday, July 12. The case was reported by Angolan authorities in the port city of Lobito, 250 miles south of the capital of Luanda, where the country's first new case in four years was reported earlier this month, said Oliver Rosenbauer, spokesperson for the WHO's polio eradication program. "Certainly they've got an outbreak," Rosenbauer told The Associated Press. "The spread of it remains to be seen." The two cases are genetically linked and it is unlikely that the second case was brought into the country separately, he said. Both cases in Angola have been tied to a strain of the virus found in India, Rosenbauer said. Investigations are continuing to determine how it made its way to southwest Africa. The Angolan Ministry of Health first contacted WHO last month after a 17−year−old girl developed paralysis in both legs. It marked the first case of polio reported in the country since 2001. Two national immunization rounds have been planned for Angola, the first to take place July 29−31 and the second August 26−28, Rosenbauer said.
Source: http://www.latimes.com/news/nationworld/world/wire/sns−ap−angola−polio,1,7637170.story?coll=sns−ap−world−headlines

24. *July 11, University of California, San Diego* — **Discovery suggests new way to fight antibiotic−resistant Staphylococcus.** Researchers at the University of California, San Diego (UCSD) School of Medicine and Children’s Hospital and Health Center, San Diego, have discovered that “Staph” bacteria use a protective golden armor to ward off the immune system, a finding with the potential to lead to new treatments for serious infections now increasingly resistant to standard antibiotics. The research focused on the major human pathogen Staphylococcus aureus and the characteristic yellow−orange color for which it is named “Staph” is the leading cause of human infections in the skin and soft tissues, bones and joints, abscesses and normal heart valves. The spread of antibiotic−resistant strains of Staph, referred to as methicillin−resistant Staphylococcus aureus, has reached epidemic proportions and poses a major threat to the public health. The UCSD team proved for the first time that the golden pigment that coats the surface of Staph is not just for decoration; rather, the molecules that give the bacteria its golden hue also help it resist killing by neutrophils, white blood cells with a front line role in immune defense against invading microbes. The scientists found that pathogenic Staph took advantage of the antioxidant effects of its carotenoid pigment to extend its own life, by inactivating chemicals deployed by neutrophils that are lethal to most bacteria.
Source: http://ucsdnews.ucsd.edu/newsrel/health/07_11_Nizet.asp

25. *June 10, Government Accountability Office* — **GAO−05−308: Federal Agencies Face Challenges in Implementing Initiatives to Improve Public Health Infrastructure.** Information technology (IT) is central to strengthening the public health infrastructure through the implementation of systems to aid in the detection, preparation for, and response to bioterrorism and other public health emergencies. Congress asked the Government Accountability Office (GAO) to review the current status of major federal IT initiatives aimed at strengthening the ability of government at all levels to respond to public health emergencies. As federal agencies work with state and local public health agencies to improve the public

health infrastructure, they face several challenges. First, the national health IT strategy and federal health architecture are still being developed; the Centers for Disease Control and Prevention (CDC) and the Department of Homeland Security (DHS) will face challenges in integrating their public health IT initiatives into ongoing efforts. Second, although federal efforts continue to promote the adoption of data standards, developing such standards and then implementing them are challenges for the health care community. Third, these initiatives involve the need to coordinate among federal, state, and local public health agencies, but establishing effective coordination among the large number of disparate agencies is a major undertaking. Finally, CDC and DHS face challenges in addressing specific weaknesses in IT planning and management that may hinder progress in developing and deploying public health IT initiatives.
Highlights: http://www.gao.gov/highlights/d05308high.pdf
Source: http://www.gao.gov/new.items/d05308.pdf

[Return to top]

Government Sector

26. *July 09, Atlanta Journal−Constitution (GA)* — **Courthouse review cites lying, apathy.** Sheriff's deputies at the Fulton County, GA, Courthouse ignored specific warnings that a prisoner was dangerous, failed to turn on a key security monitor, and lied to investigators looking into security breaches after a fatal shooting spree in March, a special commission has found. A detailed report on the March 11 shootings at the courthouse in downtown Atlanta show that mistakes made by deputies were much worse than previously reported. Several deputies interviewed during an internal affairs investigation lied about some aspect of their activities on the day Brian Nichols allegedly beat up a deputy, took her gun, killed a judge, his court reporter, and another deputy, then fled, later killing another man. The report by a committee of the Fulton County Courthouse Security Commission, which was empanelled to investigate how the courthouse shooting spree occurred, paints a picture of sloppy record−keeping, bumbling security procedures, and high−ranking officers failing to do their duty. The investigators document a pattern of incompetence, lying, absenteeism, lax security and failed leadership in the Sheriff's Department. Fulton Sheriff Myron Freeman, who appointed the investigative commission, said he would review the findings over the weekend and make a decision within a few days about any changes needed.
Source: http://www.ajc.com/metro/content/metro/atlanta/0705/09a1cour thouse.html

[Return to top]

Emergency Services Sector

27. *July 12, The Christian Science Monitor* — **Security funds reach small towns, but at a trickle.** Four years after the September 11, 2001, terrorist attacks, more than $7 billion dollars have been appropriated for the nation's first responders, yet only $1.2 billion has actually gotten to the nation's emergency personnel. In Connecticut, as in most states across the nation, much of that new homeland−security money is caught in bureaucratic bottlenecks. The causes of delay range from the need to create new departments on the state level to disperse the funds to arcane

purchasing requirements. In other cases, grants have been given, but manufacturers of security equipment, like bomb resistant robots, have large back orders, and the equipment has yet to reach firefighters. Many towns have found that while the Department of Homeland Security (DHS) offers the opportunity to buy plenty of equipment and training, they don't always have enough people to take advantage of it. In April, DHS put out its first "National Preparedness Goal," which lays out specific criteria to give the states and localities guidance on the best way to utilize their homeland−security dollars. The House has also passed a bill that would require all future homeland−security grants to be distributed based on potential terrorist risk. A similar bill is pending in the Senate.
Source: http://csmonitor.com/2005/0712/p03s01−uspo.html

28. *July 11, Associated Press* — **Las Vegas hones terrorism response skills.** Police, firefighters and state and federal emergency officials are honing their terrorism response skills over the next four days in Las Vegas, NV. As many as 78 agencies are expected to take part in several disaster scenarios, including one involving an attack on the Las Vegas Strip. Clark County health officials plan to operate a simulated casualty collection point at the Las Vegas Convention Center. Actors are playing the role of casualties. That'll be followed by a decontamination process for 500 bodies involving the county coroner and an Army Reserve unit. Some exercises will be at the Clark County Government Center. Others are at the Convention Center. That's where officials are offering a free pet microchip clinic to implant identification tags under the skin of one thousand pets brought in by their owners.
Source: http://www.kesq.com/Global/story.asp?S=3579019

29. *July 11, The Times Herald (PA)* — **Pennsylvania town stages decontamination exercise.** The Norristown, PA, Fire Department staged a simulated decontamination exercise outside the Montgomery Hospital emergency room Sunday, July 7, testing their response, equipment and training, as well as the police, hospital staff and county public safety department. In the event that the local hospital is forced to deal with an incident of bioterrorism, volatile chemical spill or even anthrax, the community needs to appreciate that the responding individuals in control of the situation know what they're doing. In Sunday's drill, the emergency personnel acted under the circumstances that a chemical contamination had occurred in Philadelphia and affected victims were seeking treatment at area hospitals outside of the city. Responding to several individuals swarming the emergency room complaining of similar symptoms, the Montgomery Hospital Emergency Incident Command System took control and contacted the fire department. On the scene outside of the emergency room, the fire department demonstrated their hazardous material training. Eight of the nine companies in the county with hospitals in their regions have been trained and given equipment for such circumstances.
Source: http://www.timesherald.com/site/news.cfm?newsid=14837518&BRD=1672&PAG=461&dept_id=33380&rfi=6

[Return to top]

Information Technology and Telecommunications Sector

30. *July 12, US−CERT* — **Technical Cyber Security Alert TA05−193A: Microsoft Windows, Internet Explorer, and Word Vulnerabilities.** Microsoft has released updates that address critical vulnerabilities in Windows, Office, and Internet Explorer. Exploitation of these

vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code with the privileges of the user. If the user is logged on with administrative privileges, the attacker could take control of an affected system.
Microsoft has provided the updates for these vulnerabilities:
http://www.microsoft.com/technet/security/bulletin/ms05−jul. mspx
Source: http://www.us−cert.gov/cas/techalerts/TA05−193A.html

31. *July 11, Secunia* — **phpWebSite PEAR XML_RPC PHP code execution.** A vulnerability has been reported in phpWebSite, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability has reportedly been fixed in the CVS repository.
Source: http://secunia.com/advisories/16001/

32. *July 11, Security Focus* — **ISC DHCPD remote format string vulnerability.** A remote format string vulnerability is reported in the ISC DHCPD server package. User supplied data is logged in an unsafe fashion. Exploitation of this vulnerability may result in arbitrary code being executed by the DHCP server. Although unconfirmed it is conjectured that this issue may only be exploitable when debugging functionality is enabled. It is reported that the vendor has released an update to address this vulnerability. This update is reported to be located at: ftp://ftp.isc.org/isc/dhcp/dhcp−3.0.2rc1.tar.gz
Source: http://www.securityfocus.com/bid/11591/info

33. *July 11, FrSIRT* — **MMS Ripper (MMSRIP) MMST streams heap overflow vulnerability.** A vulnerability was identified in MMS Ripper, which could be exploited by attackers to execute arbitrary commands. This flaw is due to a heap overflow error in the "mms_interp_header()" function when handling multiple stream IDs, which may be exploited via a malicious server to compromise a vulnerable system. Users should upgrade to MMS Ripper version 0.6.4 or later: http://nbenoit.tuxfamily.org/projects/mmsrip/
Source: http://www.frsirt.com/english/advisories/2005/1043

34. *July 11, FrSIRT* — **SPiD "lang_path" remote PHP file inclusion vulnerability.** A vulnerability was identified in SPiD, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in "lang.php" when processing a specially crafted "lang_path" parameter, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/1041

35. *July 07, Secunia* — **zlib "inftrees.c" buffer overflow vulnerability.** A vulnerability has been reported in zlib, which can be exploited by malicious people to conduct a DoS (Denial of Service) against a vulnerable application, or potentially to execute arbitrary code. The vulnerability is caused due to a boundary error in "inftrees.c" when handling corrupted compressed data streams. This can be exploited to crash any application that uses the zlib library, or potentially to execute arbitrary code with privileges of the vulnerable application. The vulnerability has been reported in version 1.2.2. Prior versions may also be affected. No updates are currently available from the vendor, but several Linux distributions have issued updated packages.
Source: http://secunia.com/advisories/15949/

36. *July 06, Security Focus* — **McAfee IntruShield Security Management System multiple vulnerabilities.** McAfee IntruShield Security Management System is susceptible to multiple vulnerabilities. The first two issues are cross−site scripting vulnerabilities in the 'intruvert/jsp/systemHealth/SystemEvent.jsp' script. These issues are due to a failure of the application to properly sanitize user−supplied data prior to utilizing it in dynamically generated HTML. The next two issues are authorization bypass vulnerabilities leading to information disclosure and the ability to acknowledge, de−acknowledge, and delete security alerts. These vulnerabilities require a valid user account in the affected application. \Users of affected packages should contact the vendor for further information.
Source: http://www.securityfocus.com/bid/14167/info

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 reports a working public exploit for a vulnerability in a common PHP extension module (XML−RPC) that could allow a remote attacker to execute code of their choosing on a vulnerable system. Any application, typically web−based, that uses a flawed XML−RPC PHP implementation is vulnerable to exploitation. XML−RPC allows software to make procedure calls over the Internet typically using HTTP and XML. A remote attacker could exploit the XML−RPC vulnerability to execute PHP code of their choosing. The code would be executed in the context of the server program that runs the corresponding web−based application. More information about this vulnerability can 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 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 27015 (halflife), 139 (netbios−ssn), 80 (www), 4672 (eMule), 135 (epmap), 53 (domain), 32775 (sometimes−rpc13) 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

37. *July 12, CNN* — **Explosions at Spanish power plant.** Four explosions struck a new, soon−to−be−operational electrical power plant in northern Spain on Tuesday, July 12, shortly after warning calls were made in the name of the Basque separatist group ETA, said a Basque regional police spokesperson. There was no immediate confirmation of injuries, and damage was being evaluated, the spokesperson said. After the warning calls to the Basque newspaper Gara and to the Basque emergency road service DYA, police rushed to the plant, in the Basque city of Amorebieta, and evacuated the workers. The explosions occurred in quick succession between 2:05 pm and 2:15 pm local time. The gas−fired thermal power plant is in a testing phase and not yet on line. ETA, listed as a terrorist group by the United States and the European Union, is blamed for more than 800 killings in its 37−year fight for Basque independence in northern Spain.
Source: http://www.cnn.com/2005/WORLD/europe/07/12/spain.blasts/index.html?section=cnn_latest

[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.