Department of Homeland Security Daily Open Source Infrastructure Report for 18 July 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Washington Post reports hundreds of surveillance cameras and sensors to detect intruders will be installed along a freight rail line that winds through the District of Columbia and passes within three blocks of the U.S. Capitol. (See item 8)

- The Houston Chronicle reports a Texas State Auditor's Office report has revealed that Texas officials still rely on an antiquated computer system and incomplete information to keep track of the state's livestock, including animals exposed to disease. (See item 17)

- The Associated Press reports more than 2,000 school bus drivers and managers across Texas are in a School Bus Watch program learning how to deal with possible terrorism. (See item 34)

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 15, CNN* — **Wind farms could meet energy needs.** Wind power could generate more than enough sustainable electricity to meet global energy needs, according to new research. Scientists at Stanford University have produced a world map that plots wind power potential for the first time. They say that harnessing even 20 percent of that energy would produce eight times more electricity than the world consumed in 2000. "The main implication of this study is

that wind, for low−cost wind energy, is more widely available than was previously recognized," said Cristina Archer, formerly of Stanford's Department of Civil and Environmental Engineering. Archer and colleague Mark Jacobsen collected wind−speed measurements from 7,500 surface stations and 500 balloon−launch stations to determine wind speeds at 300 feet −− the height of modern turbines. Archer and Jacobsen, whose research is published in the Journal of Geophysical Research−Atmospheres, estimate that locations with sustainable winds could produce approximately 72 terawatts −− or 72 trillion watts −− a year. It would take more than 500 nuclear power stations to generate a terawatt and in 2000 the world consumed just 1.8 terrawatts in total.
Research abstract: http://www.agu.org/pubs/crossref/2005/2004JD005462.shtml
Source: http://www.cnn.com/2005/TECH/science/07/15/wind.power/index.html?section=cnn_latest

2. *July 15, Salt Lake Tribune (UT)* — **Department of Transportation prepares for nuclear hauls to temporary storage site in Utah.** The Department of Transportation (DOT) is making preparations for its role in overseeing shipments of spent nuclear fuel to Private Fuel Storage's proposed nuclear waste dump in Utah. The department asked Congress to approve four new staff positions at a cost of about $100,000 each, who would review transit plans for the waste and ensure they comply with existing regulations governing hazardous materials shipments. The department's request indicates steps are already being taken to prepare for shipments to the waste dump, even though the Nuclear Regulatory Commission (NRC) has not yet granted a license to the facility. A license application filed by Private Fuel Storage, a group of electric utilities, is in its final stages of review and a decision is expected by the end of the summer. Private Fuel Storage plans to store 44,000 tons of high−level waste in steel and concrete casks on the Skull Valley Band of Goshutes Indian Reservation, UT, until the Department of Energy (DOE) opens a permanent repository, presumably at Yucca Mountain, NV.
Source: http://www.sltrib.com/ci_2861994?rss

3. *July 14, Brick Township Bulletin (NJ)* — **New Jersey mayor petitions for change in relicensing rules.** New Jersey's Oyster Creek power plant has been in operation since 1969 and is the oldest large−scale commercial nuclear reactor in the U.S. The plant’s owner, Exelon Corporation, is expected to apply for a 20−year license extension with the Nuclear Regulatory Commission (NRC) to keep the plant running until 2029. The plant’s current license expires in 2009. New Jersey Mayor Joseph Scarpelli said he will petition the NRC to change their requirements for renewal of the operating license. He said the requirements need to be amended because otherwise, Oyster Creek’s relicensing will be based on standards when the plant first opened — 36 years ago. The population growth is one of the biggest changes in Ocean County, NJ, during the past three decades that the NRC should take into account, Scarpelli said. However, the mayor said he believes the plant would not pass inspection if the NRC adopts the additions he’s proposed. “The NRC should be the toughest agency in Washington [D.C.],” Scarpelli said.
Source: http://bulletin.gmnews.com/news/2005/0714/Front_page/021.htm l

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

4. *July 15, Government Accountability Office* — **GAO−05−681: Industrial Security: DoD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient (Report).** The Department of Defense (DoD) is responsible for ensuring that U.S. contractors safeguard classified information in their possession. DoD delegates this responsibility to its Defense Security Service (DSS), which oversees more than 11,000 contractor facilities that are cleared to access classified information. Some U.S. contractors have foreign connections that may require measures to be put into place to reduce the risk of foreign interests gaining unauthorized access to classified information. In response to a Senate report accompanying the National Defense Authorization Act for Fiscal Year 2004, the Government Accounting Office (GAO) assessed the extent to which DSS has assurance that its approach provides sufficient oversight of contractors under foreign ownership, control, or influence (FOCI). GAO recommends that DoD direct DSS to improve data collection and analysis of FOCI transactions and protective measures and direct DSS to systematically assess the effectiveness of the FOCI process to reduce risk of foreign interests gaining unauthorized access to classified information. DSS should formulate a human capital strategy and plan to evaluate whether its staff need better information, training, and tools to perform FOCI responsibilities. DoD did not concur with GAO's recommendations and stated the process is sufficient.
Highlights: http://www.gao.gov/highlights/d05681high.pdf
Source: http://www.gao.gov/new.items/d05681.pdf

[Return to top]

Banking and Finance Sector

5. *July 16, Washington Post* — **Money laundering enforcement slow and weak, review finds.** Federal bank examiners have not acted quickly or strongly enough in enforcing laws intended to prevent terrorists and other criminals from laundering money through U.S. banks, according to an internal review released on Friday, July 15, by a key bank regulatory agency. The study, which reviewed the way regulators have monitored banks with a history of inadequate controls, found that problems have been allowed to fester. Eight of the 36 banks in the sample had failed to correct problems cited by the Office of the Comptroller of the Currency (OCC), the report said. The OCC's initial actions "have not always been severe enough to ensure timely correction," and "follow−up actions have not always been timely or effective," the report by the OCC's Quality Management Division said. "There are banks supervised by the OCC with significant . . . deficiencies that have not been fully addressed," the report said. OCC spokesperson Robert M. Garsson said that "the supervisory action just hadn't been adequate to the task," but he said the agency has been making improvements. The review focused on the controls banks employ to prevent or detect money laundering and did not determine whether money laundering was actually taking place.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/15/AR2005071501847.html

6. *July 15, Kathimerini (Greece)* — **Greek charged with U.S. credit card scam.** An Athens prosecutor on Thursday, July 14, charged a 43−year−old Piraeus, Greece, man in connection with an elaborate scam through which he allegedly stole the personal details of hundreds of U.S. citizens, obtained credit cards in their names and withdrew at least $60,000. Officers from the Attica electronic crimes squad said the man had been engaged in the scam for the last 18 months, stealing information and then sending off applications for credit cards and traveler's checks to banks in the U.S. The suspect, who has not been named, had rented several properties in the U.S., to which the banks sent the cards and checks. He then paid youths, mostly students, some $300 a week to collect the mail and forward it to a post box in Piraeus, officers said. Greek police were tipped off about the scam by the FBI and launched a three−month operation to track the suspect via the Internet.
Source: http://www.ekathimerini.com/4dcgi/_w_articles_politics_10001 2_15/07/2005_58649

7. *July 14, CNET news* — **Imposter sites plague free credit report site.** A Website created by federal mandate last year to help consumers spot identity theft is opening up new avenues for fraud, according to a privacy watchdog group. The site, AnnualCreditReport.com, offers consumers free copies of their own credit reports. It was launched in December by Equifax, Experian and TransUnion, the three major credit reporting agencies in the United States, in accordance with the Fair and Accurate Credit Transactions Act of 2003. The federal law aims to quell growing concerns over privacy and disclosure of sensitive financial data. However, the online service has quickly fallen prey to imposter sites, which are designed to lure traffic from a legitimate Website by adopting a similar domain name. Imposters targeting the AnnualCreditReport.com site now number 112, according World Privacy Forum, a nonprofit based in San Diego that's studying the problem. Another 120 registered domains that aren't currently active employ the words annual credit report in some combination or are close misspellings of the official site, the group said. The privacy advocate sounded an alarm bell on Thursday, July 14, in a report that said the imposter sites "have been aggressively attempting to deceive and misdirect consumers."
World Privacy Forum report: http://www.worldprivacyforum.org/pdf/wpfcalldontclickpt2_714 2005.pdf
Source: http://news.com.com/Imposter+sites+plague+free+credit+report +site/2100−1028_3−5789299.html

[Return to top]

Transportation and Border Security Sector

8. *July 16, Washington Post* — **Cameras, sensors to line Washington, DC railway.** Hundreds of surveillance cameras and sensors to detect intruders will be installed along a freight rail line that snakes through the District of Columbia and within three blocks of the U.S. Capitol. The $9.8 million pilot project, funded by the Department of Homeland Security, is the most detailed information to surface about plans to secure the rail line. The system will include more than 300 cameras, including ones able to detect movement, according to the federal agency. Authorized trains, vehicles and personnel will be given radio frequency identification cards that will identify them as "friendlies" to the cameras and sensors. If a vehicle or individual not recognized by the system approaches the buffer zone, an alarm will sound and an alert will be sent to a District command center, according to the federal department. The rail line also will be

equipped with virtual "gates" where trains will be scanned by nuclear, biological and chemical sensors before being allowed to continue into the city, officials said. Mayor Anthony A. Williams (D) said yesterday that the project appeared to be "a step in the right direction."
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/15/AR2005071501689.html?sub=AR

9. *July 15, Government Accountability Office* — **GAO−05−663: International Air Passengers: Staffing Model for Airport Inspections Personnel Can Be Improved (Report).** While the Enhanced Border Security and Visa Protection Act repealed a 45−minute standard for inspecting international passengers, minimizing wait times at airports remains an area of concern for U.S. Customs and Border Protection (CBP). Shortly after its creation in March 2003, CBP assumed inspection functions from the Immigration and Naturalization Service, the U.S. Customs Service, and the Department of Agriculture. The new agency's priority missions are to prevent terrorism and to facilitate travel and trade. To assess CBP's efforts to minimize wait times for international air passengers while ensuring security, this report answers the following questions: (1) What are the wait times at the 20 U.S. international airports that receive most of the international traffic and what factors affect wait times? (2) What steps have airports and airlines taken to minimize passenger wait times? (3) How has CBP managed staffing to minimize wait times across airports? The Government Accountability Office (GAO) is recommending that CBP address weaknesses in its staffing model, and determine milestones for the completion of its staffing model and cross−training activities. CBP reviewed a draft of this report and concurred in part with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d05663high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−663

10. *July 15, Chicago Tribune* — **Chicago Transit Authority employee charged with bomb threat.** A Chicago Transit Authority (CTA) employee was charged Friday, July 15, with allegedly telephoning a bomb hoax that closed the CTA Brown Line for more than an hour on Sunday, July 10. Bilal Steward was charged with calling in the threat from a pay phone at the Kimball Line terminal at 8:22 a.m. (CDT) Sunday while he was working as a train operator. Steward had been placed on probation in April after he was reprimanded for excessive absenteeism and safety violations, authorities said. A criminal complaint lodged against Steward in federal court said two CTA managers at the Kimball Terminal quickly identified Steward as the caller on a tape of the threatening 911 call. The telephoned threat led the CTA and Chicago Police Department to evacuate and close the Brown Line from the Kimball Terminal to the Western Terminal for 66 minutes, authorities said. Noting that the bomb hoax came days after terrorist bombings in London's mass transit system killed dozens, Robert Grant, special agent−in−charge of the FBI in Chicago, said in a statement, "It is unconscionable to me that anyone, let alone a CTA employee, would commit such an act."
Source: http://www.chicagotribune.com/news/local/chi−050715brownline,1,7090578.story?coll=chi−news−hed

11. *July 14, Associated Press* — **United seeking $310 million increase to bankruptcy loans.** UAL, parent of United Airlines, said in court documents Thursday, July 14, that it needs another $310 million in bankruptcy loans to provide a "stable environment" as the company works on its reorganization plan. Chicago−based UAL has said it intends to emerge from bankruptcy this fall and indicated this summer that it may need additional money during the

exit process. The request, however, is separate from the airline's ongoing pursuit of exit financing. In court documents filed to the U.S. Bankruptcy Court for the Northern District of Illinois, UAL said the additional money will provide the company with time "to complete their restructuring efforts in a systematic and measured way." The money will come in the form of an increase to UAL's existing debtor−in−possession loans. The new deal between UAL and its lenders includes an extension of the maturity date through Dec. 30 and decreases the interest rate governing the loan by 0.25 percentage points. The request, which would bring the aggregate loan total to about $1.3 billion, is still subject to court approval. It is expected to be addressed at a hearing Friday. The airline's motion also includes a provision to extend the date by which the company must provide an update business plan to its lenders to August 31.
Source: http://www.usatoday.com/travel/news/2005−07−14−united−loans_ x.htm

12. *July 14, USA TODAY* — **Airport checkpoints and chokepoints.** At Miami International Airport, one of the busiest security checkpoints has only four lanes and frequent crowds. The airport has no room to add more lanes —or tables for removing items — to speed up lines. In contrast, security lines move quickly for passengers at Minneapolis−St. Paul International Airport. That's largely because, shortly after the September 11, 2001, terrorist attacks, the airport teamed with its largest carrier, Northwest Airlines, to expand screening from eight to 17 lanes. The different experiences at Miami and Minneapolis airports illustrate one of the most confounding and frustrating phenomena of post−9/11 air travel: the wild variation in the time it takes to get through security. In a USA TODAY analysis of more than five million government records, the data, collected from June 2004 through mid−May of this year, indicate that the amount of time passengers spend in lines often is determined by conditions that are apparent to airport and security officials but nonetheless can be difficult to fix. Though much needs to be done, there is a bright note: most airports −− about 75% −− almost never have lines with wait times exceeding 20 minutes, the newspaper's analysis shows.
(Graphic: comparison of busiest airports:
http://www.usatoday.com/travel/graphics/TSAdelays/flash.htm
Source: http://www.usatoday.com/travel/flights/2005−07−14−airport−ch eckpoint_x.htm

13. *July 14, Washington Post* — **Airports to expand registered traveler plan.** Frequent fliers in the Washington area could soon get a new perk at Reagan National and Dulles International airports. The airports have joined a group that seeks to expand the federal government's Registered Traveler program, which speeds passengers to the front of the security checkpoint lines in exchange for divulging personal information and passing background checks. So far, the program is available by invitation only at six airports, most of which have only one airline participating. Under the group's plan, each airport might be able to offer its own perks, such as allowing passengers to earn additional frequent−flier miles or exempting them from having to take off their shoes or remove laptops from cases. To become a member, passengers would need to provide personal information, such as dates of birth, e−mail addresses, home addresses and phone numbers, and have their fingerprints and irises digitally scanned. Airports would then submit the information to the Transportation Security Administration (TSA). If travelers pass background checks, they would receive Registered Traveler cards containing data chips with their information. The TSA has supported a Registered Traveler program for about two years, but it has had difficulty getting it off the ground.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07
/14/AR2005071401776.html?sub=AR

14. *July 14, Transportation Security Administration* — **TSA suspends 30−minute rule for Reagan National Airport.** The Transportation Security Administration (TSA) is suspending the section of a Security Directive that has required all passengers flying into and out of Ronald Reagan Washington National Airport to be seated for 30 minutes after departure or before arrival. The rule will be suspended as of 6 p.m. on Friday, July 15. Department of Homeland Security Secretary Michael Chertoff announced the 30−minute rule would be suspended when he unveiled a broad reorganization of the department Wednesday. Kenneth Kasprisin, Acting Assistant Secretary of Homeland Security for TSA, said, "Our efforts along with the cooperation of commercial airlines have brought us to the point where this rule is no longer needed. We are confident in our systematic layered approach to airline security." While the rule was valuable when applied following the 9/11 attacks, TSA's security web is far more sophisticated today and better prepared to handle security threats from passengers. Significantly enhanced layers of security range from hardened cockpit doors to advanced screening procedures and air marshals on flights.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 0149896

[Return to top]

Postal and Shipping Sector

15. *July 15, Associated Press* — **Man shoots postal worker in apparent bid to go to prison.** Two weeks ago, in Snellville, GA, William Crutchfield walked down his driveway carrying a pistol and greeted his mail carrier at the curb. He then opened fire on Earl Lazenby, drove to the police station and told the secretary, "I just shot the letter carrier." Lazenby was shot seven times, once in the arm and six times in the abdomen. On TV, Crutchfield followed the case of Eric Rudolph −− who pleaded guilty this spring in a deal that will send him to prison for life −− and wanted the same fate. "Crutchfield said that he wanted to be cared for by the federal government, that he was in poor health and wanted to be taken care of," said Atlanta postal inspector Tracey Jefferson. Crutchfield, a 60−year−old electrical contractor who lived alone, claimed $90,000 in medical debts for an unspecified ailment and feared losing his home, another postal inspector testified at his preliminary hearing.
Source: http://www.newutah.com/modules.php?op=modload&name=News&file =article&sid=59758&mode=thread&order=0&thold=0

[Return to top]

Agriculture Sector

16. *July 15, Associated Press* — **Soybean rust case worries farmers.** Soybean specialist Alan Blaine is busy trying to calm anxious farmers worried about a potential soybean rust invasion in Mississippi and its neighbors. Blaine said since soybean rust was detected the week of July 11 in a commercial field near Foley, AL, his telephone has been ringing nonstop. Mississippi farmers want to know how much of the state's 1.7 million soybean acres could be at risk. As of Thursday, July 14, no soybean rust had been found in Mississippi, Blaine said, before cautioning that recent storm conditions −− in part because of the passage of Tropical Storm

Dennis though portions of the state −− could change that status. Soybean rust, which is spread by wind−borne spores, has not caused any significant damage in the U.S. since it arrived in 2004. The disease cost farmers in Brazil about one billion dollars last year in crop losses and fungicide treatments. Soybeans represent the largest acreage of planted crops in the nation at 75 million acres. The crop is second only to corn in total value. Blaine, an extension agronomist at Mississippi State University, estimates that Mississippi's current crop is worth about $500 to $600 million.
Source: http://www.clarionledger.com/apps/pbcs.dll/article?AID=/2005 0715/BIZ/507150352/1005

17. *July 15, Houston Chronicle (TX)* — **Livestock tracking deficient, audit says.** Texas officials rely on an antiquated computer system and incomplete information to keep track of the state's livestock, including animals exposed to disease, a Texas State Auditor's Office report revealed Thursday, July 14. The audit examined records kept by the commission from September 1, 2003 to February 28, 2005. According to the audit, blood and tissue samples sent to the agency for testing were sometimes mailed late to the agency, missing a 48−hour commission deadline. It recommended that the agency have veterinarians adhere more strictly to the commission's deadlines about sample recovery. Also, some paper permits used to regulate the transportation of diseased, exposed and non−tested livestock in Texas were either missing critical pieces of information or a hard copy of the permit was nowhere to be found at the agency. A sample of 34 livestock blood tests found that owner name and address information in 29 tests were incomplete. These blood samples, collected at slaughterhouses and tested by the agency, are used to determine if an animal is diseased. Auditors also noted that until April, the commission had not applied for homeland security funding that would help pay for a better system of data keeping. Texas has 13.8 million head of cattle, about 15 percent of the nation's cattle market.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/326711 3

18. *July 14, Fort Morgan Times (CO)* — **Goss's wilt found in Colorado.** Colorado State University's (CSU) plant diagnostic clinic has verified two cases of Goss's wilt on corn in Morgan, CO. The CSU lab has also received other very likely samples from fields in Logan, Yuma, and Kit Carson, CO. Field symptoms included gray to yellow striping of the lower leaves. The margins of the spots or stripes tend to be wavy. A characteristic feature of Goss's wilt is the formation of blackish, water−soaked spots or freckles in the damaged leaf tissue. Scattered stunted plants may be present throughout the fields. These stunted plants may show an orange discoloration of the water conducting system if you slice through the stalk. Most resistant corn varieties available today have partial resistance and will not totally eliminate Goss's wilt. However using them can gradually reduce the amount of disease−laden residue for subsequent years. Historically, the serious Goss's wilt problems of the late 1970's in Colorado and Nebraska cornfields were primarily overcome through using resistant corn hybrids. Goss's wilt was virtually non−existent from 1982 to 1995.
Source: http://www.fortmorgantimes.com/Stories/0,1413,164%257E8305%2 57E2965460,00.html

[Return to top]

Food Sector

19. *July 16, Bloomberg News* — **Seafood sent to China before reaching U.S. tables.** Fish processors in the Northwest are sending part of their catch to China to be filleted or de−shelled before returning to U.S. tables. "There are 36 pin bones in a salmon and the best way to remove them is by hand," says Charles Bundrant, founder of Trident, which ships about 30 million pounds of its 1.2 billion−pound annual harvest to China for processing. "Something that would cost us one dollar per pound labor here, they get it done for 20 cents in China." Alaska and Washington have each lost about one−fifth of their processing jobs over the past decade. "It's a dying industry in the U.S.," says Tony Neves, senior vice president of Red Chamber, the second−biggest U.S. seafood company. Pacific Seafood Group, the third−biggest U.S. seafood company, started a trial six months ago to process Dungeness crabs in Qingdao, China. Crab shakers in Qingdao get $100 to $150 a month to extract meat from crab shells with pincers −− one−tenth what it might cost in the U.S. Premier Pacific Seafoods spent $10 million last year to build a new facility on its 680−foot Ocean Phoenix fishing vessel to prepare Alaskan pollock for sale to processors in China.
Source: http://seattletimes.nwsource.com/html/businesstechnology/2002384544_uschinafish16.html?syndication=rss

20. *July 15, Associated Press* — **U.S. to resume Canada cattle imports soon.** Paperwork is all that prevents truckloads of Canadian cattle from rolling into the U.S. now that a federal appeals court has lifted a ban related to mad cow disease, U.S. Department of Agriculture (USDA) Secretary Mike Johanns said Friday, July 15. Both countries had been anticipating the ruling and may be ready to resume shipments next week, Johanns told reporters in a telephone call. A three−judge panel of the 9th U.S. Circuit Court of Appeals on Thursday, July 14, unanimously overturned a Montana judge's decision that had kept the border closed. The U.S. will reopen the border to cattle younger than 30 months and expand the types of beef products that Canada is allowed to ship. Older animals are still banned because infection levels are believed to increase with age. For trade to resume, the Agriculture Department needs to issue procedures and a list of beef products allowed to cross the border, then make sure that state and federal authorities will use the guidelines to inspect shipments. The ban was costly for Canadian ranchers, who lost more than $5.7 billion, the Canadian Cattlemen's Association estimated. The U.S. banned Canadian cattle after Canada discovered its first case of mad cow disease in May 2003.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/15/AR2005071500252.html

[Return to top]

Water Sector

Nothing to report.

[Return to top]

Public Health Sector

21. *July 16, Associated Press* — **Indonesia says bird flu suspected in three deaths.** A man and his two daughters have died of suspected bird flu in Indonesia, authorities said Friday, July 15, and initial investigations showed they had no contact with poultry, raising concerns of possible

human−to−human transmission. The victims, a 38−year−old man and his two girls, ages nine and one, would be the country's first human fatalities linked to the virus. They lived in a suburb of Jakarta and all died in the last week and a half, Health Minister Siti Fadilah Supari said. Supari said the man's wife, his son and their two maids have shown no symptoms of the disease −− which include fever and respiratory problems −− and tests have been carried out on more than 300 people who were in contact with the family.
Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/11215319
47577_45/?hub=Health

22. *July 16, San Francisco Chronicle (CA)* — **Bacteria discovered in flu shots intended for European market.** Chiron Corp., which is still seeking approval to resume U.S. sales of flu vaccine from a plant that was sidelined last year by contamination, announced Friday, July 15, that similar problems have surfaced at a different factory that makes its flu shots for the European market. After finding bacteria in some vaccine lots from its plant in Marburg, Germany, the firm said it will be able to produce at most four million doses, or one−third of the 12 million shots of Begrivac it had planned to deliver to customers in Germany and the United Kingdom in the coming flu season.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2005/07/16/ BUGR8DOQTQ1.DTL

23. *July 15, Science* — **Avian influenza: who controls the samples?** At a time when averting a global influenza pandemic may depend on the rapid sharing of samples and information, researchers in developed and developing countries alike are running into roadblocks. Despite a consensus that samples of H5N1 strains should be sent to international reference labs as soon as they appear, no existing international agreement requires labs or countries to do so. Researchers have to ask individual labs and governmental authorities for samples and information. And those requests have to get to the right people. Even sending samples to the U.S. Centers for Disease Control and Prevention (CDC) and other World Health Organization (WHO) collaborating centers may not mean that samples and results get to all who want them. The collaborating centers must first report the results of any studies to the country or lab that supplied the samples; they also need the source's permission to pass samples on to third parties. Bioterror precautions also impede sharing, even with highly regarded labs. David Daigle, a spokesperson for CDC's National Center for Infectious Diseases, confirms that an initial clearance for exporting a select agent can take several months, although the agency is trying to speed the process.
Source: http://www.sciencemag.org/cgi/content/full/309/5733/372

24. *July 14, University of Washington* — **Primate virus jumps species barrier to humans for first time in Asia.** Scientists have identified the first reported case in Asia of primate−to−human transmission of simian foamy virus (SFV), a retrovirus found in macaques and other primates that so far has not been shown to cause disease in humans. The transmission of the virus from a monkey to a human took place at a monkey temple in Bali, Indonesia. "The issue of primate−to−human viral transmission has been studied extensively in Africa, largely because that is where HIV originated," explains Lisa Jones−Engel, lead author of the study. "But there has not been much work on the topic in Asia, which has huge primate diversity and large human populations." The vast majority of previous viral transmission research focused on bushmeat hunting and consumption, a practice in which local residents hunt monkeys for food. HIV is believed to have originated as simian immunodeficiency virus (SIV), and jumped the

species barrier to humans when African bushmeat hunters came into contact with blood from infected animals. Jones−Engel says, people in Asia have many other contexts in which they come into contact with primates, including animal markets, primate pet ownership, urban performing primates, and zoos. In addition, monkey temples −− places of religious worship that have become refuges for populations of primates −− are common throughout much of South and Southeast Asia.
Source: http://www.uwnews.org/article.asp?articleID=11179

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

25. *July 14, Fallon Star Press (NV)* — **Navy stages mass casualty drill.** Naval Air Station Fallon, in Fallon NV, held its first multiple−agency mass casualty disaster drill this month. According to Don Hardy, the Navy's emergency management coordinator, the exercise simulated a terrorist firing a shoulder−held rocket at a C−40 passenger aircraft that subsequently crashes into the weapons loading area on base and comes to a rest near the base theater several hundred yards away. About 30 sailors and Nevada Air National Guard personnel volunteered their time to play the role of "victim" and were made−up in paint to simulate injuries ranging from head wounds to amputations. The air station's federal fire fighters responded to the "crash site" and simulated putting out the fire and rescuing victims. Pilots and crewmen from the Reno−based Nevada Air National Guard flew a C−130 transport plane to the air station to "evacuate" victims to regional medical facilities and burn centers. "Critically" injured personnel were flown by the Air National Guard to Reno to simulate medical evacuation flights that would actually take place in the case of a real mishap. The Nevada Air National Guard's C−130s are one of the only resources in Northern Nevada that can be used for large−scale medical evacuations, according to Hardy.
Source: http://www.rgj.com/news/stories/html/2005/07/14/104098.php?sps=rgj.com&sch=Fallon&sp1=rgj&sp2=News&sp3=Fallon&sp5=FallonStarPress.com&sp6=news&sp7=local_news

26. *July 14, The Daily Times (TN)* — **Tennessee agencies take part in meth drill.** Emergency services agencies tested their skills Wednesday, July 13, during the largest decontamination exercise held in Blount County, TN. The scenario was the explosion of a meth lab. The 11 "victims" taken to Blount Memorial Hospital, including one child, weren't really hurt. Having all the county's emergency services agencies participate was essential to improve how they all function under a "unified command," according to Kelley Mure, Blount County Homeland Security Director. Emergency services in the cities and county learned more about their strengths and looked for problem areas, said Mure. Blount Memorial Hospital Security Director Mark Griffith agreed: "This is the first time in 26 years that we've had all our local emergency responders collaborate on exercise like this, and that's great cooperation that'll benefit the

community." Mure said the exercise went well overall. In the next few days, agencies will critique their performance.
Source: http://www.thedailytimes.com/sited/story/html/212192

[Return to top]

Information Technology and Telecommunications Sector

27. *July 15, Government Accountability Office* — **GAO−05−552: Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements (Report).** Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Concerned with accounts of attacks on systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act (FISMA) in 2002. In accordance with FISMA requirements that the Comptroller General report periodically to the Congress, GAO's objectives in this report are to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) the federal government's implementation of FISMA requirements. GAO recommends that the Director of the Office of Management and Budget (OMB) implement improvements in the annual FISMA reporting guidance. In commenting on a draft of this report, OMB agreed with GAO's overall assessment of information security at agencies but disagreed with aspects of our recommendations to enhance its FISMA reporting guidance.
Highlights: http://www.gao.gov/highlights/d05552high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−552

28. *July 14, TechWeb News* — **Attackers could eavesdrop on Cisco−routed VoIP calls.** Flaws in Cisco's Voice−over−Internet Protocol (VoIP) software could allow an attacker to bring down the alternative−to−traditional−telephone service, or access the server that initiates and routes Web−based calls, an Atlanta−based security firm said. According to alerts posted online by Internet Security Systems' (ISS) X−Force research team, Cisco's CallManager sports a pair of bugs that could be "reliably exploited" by hackers. The potential result: at best a denial−of−service style crash, at worst, a situation where the attacker could redirect calls at will or even eavesdrop on conversations. By sending specially crafted packets to Cisco CallManager, an attacker could create a heap overflow and crash the system or gain access. ISS said that an exploit wouldn't need any help from a user, pushing the threat into a more dangerous category. Cisco's own advisory includes details on patched editions of CallManager that are ready to download and install.
Cisco advisory: http://www.cisco.com/warp/public/707/cisco−sa−20050712−ccm.s html
Source: http://www.techweb.com/wire/security/165702369

29. *July 14, vnunet.com* — **Apple unveils OS X security patches.** Apple has released two security fixes for bugs in its OS X operating system. The first patch plugs a hole that could allow hackers to crash a system by sending a specially crafted data packet. The flaw effectively opens up the system for a denial of service attack. A security notice on Apple's Website says that the flaw affects only the 10.4 versions of OS X and will not harm computers that sit behind a

firewall or are otherwise protected through packet filtering. The other patch targets a bug in the 10.4 Tiger operating system that allows users inadvertently to overwrite standard widgets in Apple's Dashboard application. The update provides a warning when a user attempts to install a widget that has the same name as an existing one. Previously the new widget would run instead of the system widget, effectively making the original one inaccessible to the user. This latest update moves OS X 10.4 to version 10.4.2.
Mac OS X Update 10.4.2: http://www.apple.com/support/downloads/macosxupdate1042.html
Source: http://www.vnunet.com/vnunet/news/2139781/apple−issues−two−s ecurity

30. *July 14, Secunia* — **Seagull PHP Framework PEAR XML_RPC PHP code execution.** A vulnerability has been reported in Seagull PHP Framework, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability has been reported in version 0.43. Prior versions may also be affected.
Users should update to version 0.44: http://seagull.phpkitchen.com/#download
Source: http://secunia.com/advisories/16074/

31. *July 14, Security Focus* — **Sophos Anti−Virus BZip2 archive handling remote denial of service vulnerability.** Sophos Anti−Virus is prone to a remote denial of service vulnerability when it is configured to 'Scan inside archive files'. This is not a default setting. The issue exists due to failure of the software to adequately sanitize 'Extra field length' values contained in BZip2 archives. Ultimately this vulnerability may be exploited to conduct a denial of proper service for legitimate users. Attackers may leverage this issue to prevent the software from completing file scans, for files received subsequent to an attack. This may allow the attacker to bypass Anti−Virus scans. The vendor has released updates to address this issue. These updates may be automatically applied by customers that are using the EM Library or manually from Sophos.
Update: http://www.sophos.com/support/updates
Source: http://www.securityfocus.com/bid/14270/info

32. *July 14, Security Focus* — **Simple Message Board Thread.CFM Cross−Site Scripting Vulnerability.** A cross−site scripting vulnerability affects Simple Message Board. This issue is due to a failure of the application to properly sanitize user−supplied input. An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie−based authentication credentials as well as other attacks. Currently Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/14268/discuss

33. *July 14, FrSIRT* — **WPS Web−Portal−System "wps_shop.cgi" remote command execution.** A vulnerability was identified in WPS Web−Portal−System, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in the "wps_shop.cgi" script that does not properly filter a specially crafted "art" parameter, which may be exploited by remote attackers to execute arbitrary commands via the pipe character. WPS Web−Portal−System version 0.7.0 and prior The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/1099

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 buffer overflow in the zlib data compression library caused by a lack of bounds checking in the inflate() routine. If an attacker supplies the inflate()routine with a specially crafted compressed data stream, that attacker may be able to trigger the buffer overflow causing any application linked to zlib, or incorporating zlib code to crash. According to reports, the buffer overflow is caused by a specific input stream and results in a constant value being written into an arbitrary memory location. This vulnerability may be exploited locally or remotely depending on the application being attacked. This vulnerability only affects zlib versions 1.2.1 and 1.2.2. The zlib compression library is freely available and used by many vendors in a wide variety of applications. As a result, any one of these applications may contain this vulnerability. US−CERT encouraged users to contact their vendors to determine if they are vulnerable and what action to take.

Current Port Attacks

Top 10 Target Ports	1026 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 27015 (halflife), 139 (netbios−ssn), 135 (epmap), 1871 (canocentral0), 4672 (eMule), 32775 (sometimes−rpc13), 53 (domain) 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

34. *July 15, Associated Press* — **Texas school bus drivers training for terrorism.** More than 2,000 school bus drivers and managers across Texas are learning that the backpack left on the seat might be a sign of an impending terror attack. Prompted by the terrorist takeover of a school in Russia, in which more than 300 people were killed, the program School Bus Watch will eventually include 44,000 Texas school bus drivers, said Mike Martin, executive director of the National Association for Pupil Transportation. More than 600,000 drivers nationwide eventually will undergo the training, the first attempt to standardize a national program for school bus anti−terrorism training. Until now, each school district has conducted its own training. Among the groups working on school security are the Texas Department of Public Safety and trainers from Highway Watch, which has received $40 million in federal homeland security money over two years to train truckers to pass on intelligence information to the Department of Homeland Security. "Even though none of the news is indicating that a school

transport fleet is a particular target, I don't think you can underestimate the importance of taking reasonable precautions," said Bonnie Russell, executive general manager of transportation for the Houston school district. Drivers are trained to protect themselves and their human cargo and to watch for anything suspicious.
Source: http://www.dentonrc.com/sharedcontent/APStories/stories/D8BB UV800.html

35. *July 15, Telematics Journal* — **School to track buses via GPS.** New York's South Glens Falls Central School District, in partnership with local wireless services provider Nextel Partners, has announced a new pilot project to install a modem equipped with GPS (Global Positioning System) technology, camera and student tracking system on a district school bus. The initiative is the first of its kind in Upstate New York. The GPS feature enables the location and speed of the bus to be tracked in real time as it travels on its route, which covers 25 miles serving approximately 30 summer school students. The system, which is Web−based, instantly transmits longitude and latitude information to a computer, where administrators can monitor the bus's location as it picks up and drops off children along its route. A scan of student Reader Cards tracks students getting on and off the bus. Additional safety features include inside video cameras, proximity sensor in front door, rear door alarm and wireless panic button, which will enable the driver to instantly contact dispatch or other personnel in case of emergencies. "Ensuring the safety of our students is always a priority," said Dr. James McCarthy, Superintendent of the South Glens Falls Central School District, which daily transports approximately 3,500 students on bus routes covering 65 square miles during the school year.
Source: http://www.telematicsjournal.com/content/topstories/737.html

[Return to top]

General Sector

36. *July 16, Associated Press* — **California National Guard, LA Israeli Consulate warned in probe.** Law enforcement authorities warned the Israeli Consulate and California National Guard that their facilities were on a list of possible terror targets that police found recently while investigating a string of robberies, officials said Friday, July 15. "We're very concerned about it," said Maj. Jon Siepmann, the California National Guard's deputy director of communications. "There was evidence that an attack was at least being planned." Police found the list while searching the home of a man arrested last week in connection with gas station robberies in south Santa Monica Bay communities. The list included three National Guard facilities in the greater Los Angeles area, said Siepmann, who described the threat as apparently "very serious." The warnings followed the July 5 arrests by Torrance police of Gregory Vernon Patterson, 21, and Levar Haney Washington, 25, of Los Angeles, on suspicion of robbery. Both men pleaded not guilty to the charges. FBI spokesperson Laura Eimiller confirmed last week that the agency's Joint Terrorism Task Force was investigating the case.
Source: http://www.usatoday.com/news/nation/2005−07−15−calif−threats _x.htm

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

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

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.