# Department of Homeland Security Daily Open Source Infrastructure Report for 14 July 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

## Daily Highlights

- The Associated Press reports the Bank of America Corp. is starting a new online banking security system aimed at making it harder for cyber thieves to crack customer accounts. (See item 7)
- Department of Homeland Security Secretary Michael Chertoff has announced a six−point agenda for the Department, designed to ensure that the policies, operations, and structures are aligned in the best way to address the potential threats. (See item 25)
- The US−CERT has released Technical Cyber Security Alert TA05−194A: Oracle Products Contain Multiple Vulnerabilities (See item 28)
- The New York Times reports New Ipswich, New Hampshire, police arrested a Mexican immigrant, in the country illegally, and charged him with criminal trespassing. (See item 32)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 13, Bloomberg News* — **Tropical Storm Emily may threaten supplies of crude oil in Gulf of Mexico.** Disruptions to oil output and imports caused by Tropical Storm Cindy and Hurricane Dennis may have resulted in a 2.8 million−barrel drop in U.S. crude inventories last

week. ``Luckily, Hurricane Dennis missed'' the main production areas, said Craig Pennington, head energy analyst at Schroders Plc in London. ``If we have a direct hit, it won't be $60 a barrel, it will be $70.'' This statement comes amid concerns that oil supplies may be disrupted as Tropical Storm Emily threatens to become the fifth storm to enter the Gulf of Mexico since the hurricane season began last month. U.S. oil production in the Gulf of Mexico was cut 57 percent as of July 12 by Hurricane Dennis, the U.S. Minerals Management Service said. Tropical Storm Emily, which may become a hurricane as it moves across the Caribbean Sea, may reach the Gulf next week after crossing over Mexico's Yucatan Peninsula, according to the U.S. National Hurricane Center.
Source: http://www.bloomberg.com/news/markets/energy.html

2. *July 13, Moscow News (Russia)* — **Russia, U.S. to cooperate in defending nuclear facilities.** Moscow and Washington, DC will cooperate in bolstering the security of nuclear facilities against terror attacks, according to Alexander Rumyantsev, the head of Russia's federal atomic agency, Rosatom. Russian and U.S. nuclear and defense specialists, as well as diplomats from both sides, have worked for three months to devise measures aimed at strengthening checks on radioactive material and sensitive technology, Rumyantsev reported. The cooperation plan has been sent to President Bush and Russian President Vladimir Putin, who first announced the idea at their February summit in the Slovak capital, Bratislava. Rumyantsev also raised the possibility of joint U.S.−Russian rapid reaction units to ensure nuclear security in the two former Cold War nuclear foes.
   Source: http://www.mosnews.com/news/2005/07/13/rususnuclear.shtml

3. *July 13, KCRA−3 (CA)* — **Near−record power usage expected in California.** Temperatures in the Central Valley and other parts of the California are topping temperatures of 100 degrees. The extreme high temperatures during the summer in States such as California have officials concerned about the demand for power. California officials said although demand for energy is high, there will be no electrical emergency unless a power plant goes down. Officials stress energy conservation is very important in order to avoid electrical shortages.
   Source: http://www.thekcrachannel.com/weather/4717469/detail.html

4. *July 12, KOB−TV (NM)* — **Energy demands increase in New Mexico.** After a Westside substation in New Mexico shut itself down last weekend because of demand on the electricity delivery system, the Public Service Company of New Mexico (PNM) has installed a mobile substation to help bear the load. PNM officials report that Albuquerque, NM, is using more power than ever, and nowhere is the growth greater than on the Westside. Last weekend, PNM set an all time record for power usage at 1,729 megawatts and the growth is expected to continue. "We've got more customers than ever before and customers are actually using more power," says Don Brown of PNM. PNM had planned on adding a Westside substation in 2007, but now is trying to move that schedule ahead so the new substation will be ready next summer. In the meantime, a mobile substation was attached to the Westside grid Tuesday, July 12. The mobile substation is expected to be online Thursday, July 14. Until then, PNM has rerouted power to other stations in the area in order to avoid another power outage.
   Source: http://www.kobtv.com/index.cfm?viewer=storyviewer&id=20408&cat=NMTOPSTORIES

5.

*July 12, NBC15 (WI)* — **Potential power problems in Wisconsin.** A power outage July 12 in Madison, WI, follows a July 10 outage in Fitchburg, WI. Both are followed by concerns regarding the reliability of Dane County's electricity. "Electricity usage in Dane County is growing much faster than areas in the rest of the state," says Annemarie Newman, a spokesperson for American Transmission Company, which owns roughly 8,900 transmission lines. Newman says countywide consumption is growing twice as fast as the state average, and in Southern Dane county, growth is three to four as fast as the statewide average. Early next year, the American Transmission Company is scheduled to begin construction of a new transmission line with the intent to alleviate this problem. While this will help meet the rising need for electricity in the area, that need will continue to rise, according to Newman.
Source: http://nbc15.madison.com/news/headlines/1682587.html

[Return to top]

## Chemical Industry and Hazardous Materials Sector

6. *July 13, Government Accountability Office* — **GAO−05−458: Chemical Regulation: Options Exist to Improve EPA's Ability to Assess Health Risks and Manage Its Chemical Review Program (Report).** Chemicals play an important role in everyday life, but some may be harmful to human health and the environment. Chemicals are used to produce items widely used throughout society, including consumer products such as cleansers, paints, plastics, and fuels, as well as industrial solvents and additives. However, some chemicals, such as lead and mercury, are highly toxic at certain doses and need to be regulated because of health and safety concerns. In 1976, the Congress passed the Toxic Substances Control Act (TSCA) to authorize the Environmental Protection Agency (EPA) to control chemicals that pose an unreasonable risk to human health or the environment. The Government Accountability Office (GAO) reviewed EPA's efforts to (1) control the risks of new chemicals not yet in commerce, (2) assess the risks of existing chemicals used in commerce, and (3) publicly disclose information provided by chemical companies under TSCA. GAO recommends that the Congress consider providing EPA additional authorities under TSCA to improve its ability to assess chemical risks and that the EPA Administrator take several actions to improve EPA's management of its chemical program. EPA did not disagree with GAO's recommendations but provided substantive comments.
Highlights: http://www.gao.gov/highlights/d05458high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−458

[Return to top]

## Defense Industrial Base Sector

Nothing to report.
[Return to top]

## Banking and Finance Sector

7.

*July 13, Associated Press* — **Bank of America adds new online security.** Stung by recent high−profile security breaches, Bank of America Corp. is rolling out a new online banking security system aimed at making it harder for cyber thieves to crack customer accounts. The bank leads the U.S. market with 13.2 million online banking customers and 6.4 million people who pay bills online. Bank of America launched its new online security system, called SiteKey, last month in Tennessee. It is being rolled out this week in Virginia, Maryland and Washington, DC, and should be available nationwide by the fall. Instead of the traditional user name−password setup, SiteKey users select one of a thousand different images, write a brief phrase and pick three challenge questions. The challenge questions −− all things that only the customer would be able to provide, such as the year and model of their first car −− are then used along with a customer ID and a passcode to guard access to the account. The system also allows customers to verify that they are indeed at Bank of America's Website when they log on for online banking.
Source: http://www.nytimes.com/aponline/technology/AP−Bottom−Line−BofA−Online−Security.html?

8. *July 13, Washington Post* — **Virginia official accused in identification fraud probe.** The manager of the Virginia Department of Motor Vehicles (DMV) office at Springfield Mall in Northern Virginia was charged on Tuesday, July 12, with selling driver's licenses to illegal immigrants and others for up to $3,500 apiece. The arrest of Francisco J. Martinez marked the second time in two years that a Northern Virginia DMV employee was accused of fraudulently selling licenses for cash. A similar scheme two years ago at the DMV office in Tysons Corner led to the guilty pleas of two employees. Federal prosecutors in Alexandria charged Martinez with one count of conspiracy to commit identification fraud. Virginia licenses were issued to at least 40 people who were either illegal immigrants or whose driving privileges had been suspended, prosecutors said. The case is the latest in a federal crackdown on document and identity fraud in Virginia since the September 11, 2001, attacks on the World Trade Center and Pentagon. Seven of the 19 hijackers in the attacks had fraudulently obtained Virginia documents.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/12/AR2005071201421.html

9. *July 13, The Arizona Republic* — **Medical firm's files with personal data stolen.** The personal information of 57,000 Blue Cross Blue Shield of Arizona customers was stolen from a Phoenix, AZ−based managed care company. Arizona Biodyne, an affiliate of Magellan Health Services that manages behavioral health for Blue Cross of Arizona, on Friday, July 8, began notifying customers and providers whose information was lost in the latest theft in which financial, personal or medical records were taken. The stolen information included policyholders' addresses, phone numbers, Social Security numbers and dates of birth. They also contained partial treatment histories for some patients and certain information about the doctors who provided that care, Biodyne spokesperson Erin Somers said.Most of the people at risk from the Biodyne theft live in Arizona. It is unclear whether the thieves knew what they had when they stole a safe. Biodyne reported to police on June 29 that a safe containing computer backup tapes was stolen from its office. Biodyne and Blue Cross said it is not clear whether the people who took the safe did so with the intent to use people's personal information.
Source: http://www.azcentral.com/business/articles/0713biodyne13.htm l

**10.** *July 12, KGBT 4 (TX)* — **Identity thieves swipe victims' bank account information to steal gas.** Police in Mission, TX, have arrested two of the five people wanted in what investigators are calling a well−orchestrated identity theft scheme. Arturo Duque Aguilar and Raul Lerma Montelongo and three other suspects are accused of downloading bank account details and storing the personal information on the magnetic strip of a gift card. Police say the men would take those gift cards with someone else's bank account, swipe them at gas pumps and then fill up at gas stations. However, it wasn't just an ordinary fill−up, they had a truck loaded with three to six 55−gallon barrels and they would allegedly fill them with diesel and then sell it. Investigators started getting calls from customers about the suspicious activity on their accounts, mostly from customers with Chase Bank. That's when investigators starting visiting the stores where these illegal transactions occurred. The K−mart gift card was most commonly used and the U.S. Secret Service is trying to determine why.
Source: http://www.team4news.com/Global/story.asp?S=3584571&nav=0w0v c2xD

[Return to top]

## Transportation and Border Security Sector

**11.** *July 13, Department of Transportation* — **Loan to help short line railroad in Texas.** The Tex−Mex Railroad, a short line connecting the United States to Mexico, has won approval of a $50 million loan it will use for major safety and infrastructure projects in the wake of growing cross border trade. The loan from the Federal Railroad Administration (FRA) will increase efficiency by allowing Tex−Mex to operate at higher track speeds, and increase capacity to accommodate growing freight rail traffic along its busy North American Free Trade Agreement corridor. The loan will help upgrade 146 miles of track, rehabilitate 26 bridges, construct two new sidings and lengthen one, and replace 75,000 crossties. Two rail yards, at Laredo and Corpus Christi, also will be upgraded. In addition, a portion of the loan will be used to refinance prior debt incurred for previous capital investment projects. The loan is being made under the Railroad Rehabilitation and Improvement Financing program administered by the FRA. This program assists short line and regional railroads to acquire, improve, or rehabilitate rail equipment and infrastructure. The Tex−Mex railroad is now a part of the Kansas City Southern Railway (KCSR) network. It serves mainly as a bridge railroad to move traffic and make connections between KCSR, Union Pacific, BNSF Railway, and Transportacion Ferrovaiaria Mexicana located in Mexico.
Source: http://www.dot.gov/affairs/fra1705.htm

**12.** *July 13, Associated Press* — **Northwest, mechanics seek end to mediated talks.** A Northwest Airlines executive said it's clear that negotiations with the airline's mechanics' union over pay cuts have stalled, and the National Mediation Board should release the two sides from mediated talks. A formal release would prompt a 30−day countdown toward a strike or a lockout — or a deal. Both sides have begun preparations for a strike. In a July 7 letter to the board, Northwest Airlines said "it is now clear that both parties to these negotiations believe it is time to issue a release." The airline made a formal request to that effect in May, but was quickly denied. Last week, the Aircraft Mechanics Fraternal Association filed its own request for release from the mediated talks. It was to that petition that Julie Hagen Showers, NWA vice president for labor relations, responded. The company is seeking $1.1 billion in annual labor cost savings. It has gotten a total of $300 million from pilots and managers, and is seeking $148 million from flight

attendants, according to their union.
Source: http://www.usatoday.com/travel/news/2005−07−12−nwa−mechanics _x.htm

**13.** *July 13, USA TODAY* — **JetBlue makes move into Newark.** Discounter JetBlue is poised to become the only low−fare carrier with service from all three New York City airports after announcing on Tuesday, July 12, plans to begin operating from Newark Liberty in New Jersey. New York−based JetBlue said it will launch service on October 5 from Newark to five Florida destinations: Fort Lauderdale, West Palm Beach, Orlando, Tampa, and Fort Myers. And starting in November, it will fly Newark to San Juan, Puerto Rico. JetBlue's announcement is the latest sign that low−fare carriers are penetrating even the largest and most entrenched air markets. s Greater New York is the world's largest air market for air travelers starting or ending a trip. It accounts for about $14 billion a year in airline revenue. At Newark, JetBlue will be taking on Houston−based Continental Airlines, which operates a huge hub and controls nearly 70% of all flights. Continental is the New York region's top airline in terms of domestic passengers.
Source: http://www.usatoday.com/travel/news/2005−07−12−jetblue−usat _x.htm

**14.** *July 13, New York Times* — **Funds will be there when technology is, transit chief says.** The head of New York's Metropolitan Transportation Authority (MTA) acknowledged on Tuesday, July 12, that the agency had been slow to spend more than $600 million budgeted for counterterrorism efforts, but he maintained that a lack of reliable technologies had made it difficult to determine how best to defend the transit network against a potential attack. "The easy way out would be to spend the money quickly, without a thorough analysis of the cost and benefit," the chairman, Peter S. Kalikow, said in an interview. "The technology for this kind of stuff is still emerging." But Kalikow, who has rarely spoken publicly about specific attempts the authority has made to better protect the city's subways, buses, and bridges, conceded that over the nearly four years since 9/11, some time had been wasted in taking action. The deadly subway and bus attacks in London last week drew renewed attention to transit security in New York City, which has the largest mass transit system in the United States. The authority has added some 200 officers to its police force, which protects two commuter railroads as well as Pennsylvania Station and Grand Central Terminal.
Source: http://www.nytimes.com/2005/07/13/nyregion/13mta.html

**15.** *July 13, Government Accountability Office* — **GAO−05−896T: Aviation Security: Better Planning Needed to Optimize Deployment of Checked Baggage Screening Systems (Testimony).** Mandated to screen all checked baggage using explosive detection systems at airports by December 31, 2003, the Transportation Security Administration (TSA) deployed two types of screening equipment: explosives detection systems (EDS), which use computer−aided tomography X−rays to recognize the characteristics of explosives, and explosives trace detection (ETD) systems, which use chemical analysis to detect traces of explosive material vapors or residues. This testimony discusses (1) TSA's deployment of EDS and ETD systems and the impact of initially deploying these systems, (2) TSA and airport actions to install EDS machines inline with baggage conveyor systems, and the federal resources made available for this purpose, and (3) actions taken by TSA to optimally deploy checked baggage screening systems. In a prior report, the Government Accountability Office (GAO) recommended that TSA systematically evaluate baggage screening needs at airports, including identifying the costs and benefits of installing in−line EDS systems or stand−alone

EDS machines in lieu of ETD machines, and prioritizing those airports where TSA would benefit by such actions. DHS generally concurred with the recommendations and described its corrective actions to address the issues identified.
Highlights: http://www.gao.gov/highlights/d05896thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−896T

16. *July 13, Government Accountability Office* — **GAO−05−834T: Commercial Aviation: Structural Costs Continue to Challenge Legacy Airlines' Financial Performance (Testimony).** Since 2001, the U.S. airline industry has confronted unprecedented financial losses. Two of the nation's largest airlines −− United Airlines and US Airways −− went into bankruptcy, terminating their pension plans and passing the unfunded liability to the Pension Benefit Guaranty Corporation (PBGC). PBGC's unfunded liability was $9.6 billion; plan participants lost $5.2 billion in benefits. Considerable debate has ensued over airlines' use of bankruptcy protection as a means to continue operations, often for years. Many in the industry and elsewhere have maintained that airlines' use of this approach is harmful to the industry, in that it allows inefficient carriers to reduce ticket prices below those of their competitors. This debate has received even sharper focus with pension defaults. Critics argue that by not having to meet their pension obligations, airlines in bankruptcy have an advantage that may encourage other companies to take the same approach. The Government Accountability Office (GAO) is completing a report for the Committee due later this year. Today's testimony presents preliminary observations in three areas: (1) the continued financial difficulties faced by legacy airlines, (2) the effect of bankruptcy on the industry and competitors, and (3) the effect of airline pension underfunding on employees, airlines, and the PBGC.
Highlights: http://www.gao.gov/highlights/d05834thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−834T

[Return to top]

## Postal and Shipping Sector

Nothing to report.

[Return to top]

## Agriculture Sector

17. *July 13, Associated Press* — **U.S. tries again to end ban on Canadian cattle.** The U.S. Department of Agriculture insists it is safe to resume importing Canadian cattle, despite a ruling by a Montana federal judge who sided with ranchers warning about economic and health consequences from a potential mad−cow outbreak in the U.S. A panel from the San Francisco, CA, based Ninth U.S. Circuit Court of Appeals travels to Seattle, WA, on Wednesday, July 13, to hear the federal government's challenge to the judge's ruling. The dispute between ranchers −− whose profits have improved slightly without Canadian competition −− and feedlots and packers −− which have fewer cattle to slaughter without Canadian supplies −− became more complicated two weeks ago, when the government revealed that a 12−year−old animal born in Texas tested positive for mad−cow disease. Ranchers, who back the ban put in place after a Canadian−born cow tested positive for mad−cow disease on a Washington farm in 2003, said

the infected Texas cow shows the continued need for a closed border, to prevent an epidemic. Philip Olsson of the National Meat Association, a U.S. trade group representing packers, processors, equipment manufacturers, and suppliers, said the Texas cow deflates the ranchers' argument that consumers would lose their appetite for U.S. meat if Canadian cattle were allowed in.
Source: http://www.theglobeandmail.com/servlet/story/RTGAM.20050713.wcoww0713/BNStory/International/

**18.** *July 06, State of Colorado Department of Agriculture* — **Vesicular Stomatitis found in Colorado.** Colorado has become the fifth state in the country to have a confirmed case of vesicular stomatitis virus (VSV). A six−year−old horse in Delta County tested positive for the disease, and the premise has been placed under quarantine. VSV can have severe economic impact on livestock owners, especially in the dairy industry, said Wayne Cunningham, state veterinarian at the Colorado Department of Agriculture. The disease usually doesn't result in an animal's death, but the main reason we watch it closely is due to fact that the symptoms closely resemble foot−and−mouth disease, which is much more economically devastating. Vesicular stomatitis is a viral disease that causes painful lesions around an infected animal's mouth, nostrils, teats and hooves, symptoms similar to foot−and−mouth disease. Only laboratory tests can differentiate the diseases. VSV primarily affects cattle, horses, and swine. These blisters enlarge and break, leaving raw tissue that is so painful infected animals generally refuse to eat or drink and show signs of lameness. Severe weight loss usually follows.
Source: http://www.ag.state.co.us/commissioner/press/2005/VSpositive .html

[Return to top]

## Food Sector

**19.** *July 13, Agricultural Research Service* — **New test leaves fewer places for bacteria to hide.** Identifying harmful yeasts and bacteria is faster, easier, and more sensitive than current detection methods, thanks to a new test by Agricultural Research Service (ARS) scientists. As a research tool, the new method's use could shed light on what makes some strains of the bacterium Listeria monocytogenes more pathogenic than others. In food−processing applications, the test's use could help redirect critical−control−point programs to better prevent contamination at manufacturing plants. Listeria's disease−causing strains are the leading cause of food recalls due to microbial contamination. Pulsed−field gel electrophoresis (PFGE) is considered the gold standard for genetically identifying Listeria bacteria that cause food poisoning. But it's difficult to run and time−consuming. The new test can be performed in a single day and distinguishes one Listeria strain from another based on nucleotide variations in their genes.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

**20.** *July 11, Food and Agriculture Organization* — **Codex adopts more than twenty food standards.** The Codex Alimentarius Commission (CAC) adopted more than 20 new and amended food standards during its annual meeting, the food standards body announced Monday, July 11. Some 120 countries were represented at this year's Codex session, plus the European Community, a member organization. Codex is an international food standards−setting body established by the United Nations' Food and Agriculture Organization (FAO) and the

World Health Organization (WHO). It has 172 members, all of which are members of FAO or WHO or both. The CAC adopted global guidelines for vitamin and mineral food supplements. The guidelines recommend labeling that contains information on maximum consumption levels of vitamin and mineral food supplements. Codex tentatively agreed to a task force addressing antimicrobial resistance. A formal decision is set for next year. WHO, FAO and the World Organization for Animal Health (OIE) have developed guidelines for the prudent use of antimicrobials in treatment of human illnesses and animal production, which the task force will carry forward to ensure food safety. In other decisions, the CAC decided to split the Codex Committee on Food Additives and Contaminants into separate committees beginning in 2007, in order to deal more effectively with each issue.
Source: http://www.fao.org/newsroom/en/news/2005/105110/index.html

[Return to top]

# Water Sector

Nothing to report.

[Return to top]

# Public Health Sector

**21.** *July 13, Los Angeles Times (CA)* — **California woman tests positive for West Nile virus.** A Yucaipa, CA, woman has tested positive for West Nile virus, San Bernardino County's first confirmed human case this year and the state's third, health officials said Tuesday, July 12. The 39−year−old woman suffered fever, aches, fatigue, and a rash in early July, but was not hospitalized and is recovering. California reported two other human cases in late June: a Tulare County man and a teenager from the Banning area in Riverside County.
Source: http://www.latimes.com/news/local/state/la−me−rbriefs13.1jul13,1,5205128.story?coll=la−news−state

**22.** *July 13, Associated Press* — **Thousands of Pennsylvania hospital patients contracted infections.** More than 11,600 patients contracted infections during hospital stays in Pennsylvania last year −− and nearly 1,800 of them died, according to a new report by a state agency that tracks health care trends. Pennsylvania is one of at least a half−dozen states that require hospitals to report information on infections, and it is the first state to publicize its findings. Hospital−acquired infections in Pennsylvania added two billion dollars to hospital costs and extended hospital stays by 205,000 days last year, according to the report by the Pennsylvania Health Care Cost Containment Council. Officials at the council said they suspect the actual incidence of infection is higher because of seeming inconsistencies in the quarterly reports on four types of infections that hospitals were required to file last year. The report is the council's first attempt to illustrate the problem since the state adopted reporting requirements in 2003. It is based on an analysis of nearly 1.6 million admissions to 173 general acute care hospitals in 2004.
Pennsylvania Health Care Cost Containment Council: http://www.phc4.org/
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/13/AR2005071300272.html

**23.** *July 13, Seattle Times (WA)* — **Vaccine drives down hepatitis A infections.** The rate of hepatitis A infections in the U.S. has shrunk by 76 percent since the beginning of a vaccination program in 1999 targeting children in 17 high−risk states. The program has driven the rate of infection down to 2.6 cases per 100,000 people, or 7,653 cases, in 2003, the latest year for which figures are available. That is the lowest rate since monitoring of the disease began in the 1960s. The program's biggest impact has been on children ages two to nine. Their infection rate nationwide has dropped 89 percent in the past six years, from 18.1 cases per 100,000 children to two cases per 100,000. A decline of 84 percent occurred among people 10 to 18. Hepatitis A is a liver disease that causes fever, nausea, abdominal discomfort, and jaundice. It is rarely fatal.
Source: http://seattletimes.nwsource.com/html/nationworld/2002377291_hepatitis13.html

**24.** *July 13, Agence France Presse* — **China's migratory birds carry a more deadly avian flu strain.** Wild birds in northwest China carry a more deadly strain of the H5N1 bird flu virus and pose a global threat as they begin their summer migrations. So far, some 6,000 birds in Qinghai province's "bird island" −− a sanctuary with some 100,000 migratory birds −− have died from an outbreak of avian influenza discovered in May. Chinese scientists who recently tested the virus samples and completed gene sequencing said the strain in the outbreak appeared different and more pathogenic than strains in previous outbreaks, the Wenhuibao newspaper said Wednesday, July 13. The virus killed chickens within 20 hours and mice within three days during laboratory experiments, the report quoted scientists as saying. "The results show that this new strain of H5N1 is very harmful," said Gao Fu, director of the Chinese Academy of Science's microbiology research institute. "The deadliness of the virus far exceeds that of the virus strains previously found in water fowl in northern China." World Health Organization officials had said last month they also believed the virus to be more lethal than previous strains as it had infected the largest flock of migratory birds ever. Species of wild birds previously not affected fell sick this time.
Source: http://news.yahoo.com/s/afp/20050713/hl_afp/healthchinaflu_0 50713115250

[Return to top]

## Government Sector

**25.** *July 13, Department of Homeland Security* — **Six−point agenda for Department of Homeland Security.** Department of Homeland (DHS) Security Secretary Michael Chertoff on Wednesday, July 13, announced a six−point agenda for the Department of Homeland Security designed to ensure that the Department's policies, operations, and structures are aligned in the best way to address the potential threats −− both present and future −− that face the nation. "Our Department must drive improvement with a sense of urgency. Our enemy constantly changes and adapts, so we as a Department must be nimble and decisive," said Chertoff. Today's announcement reflects conclusions drawn as a result of the Second Stage Review, a careful study of the Department's programs, policies, operations and structure. The Review examined nearly every element of the Department of Homeland Security in order to recommend ways that DHS could better manage risk in terms of threat, vulnerability and consequence; prioritize policies and operational missions according to this risk−based approach; and establish a series of preventive and protective steps that would increase security

at multiple levels. The Secretary also announced details of his proposal for realigning the Department of Homeland Security to increase its ability to prepare, prevent, and respond to terrorist attacks and other emergencies. These changes will better integrate the Department, giving DHS employees better tools to help them accomplish their mission.
Organization chart: http://www.dhs.gov/dhspublic/interweb/assetlibrary/DHSOrgCharts0705.pdf
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0703.xml

[Return to top]

## Emergency Services Sector

**26.** *July 12, Government Accountability Office* — **GAO−05−894T: Flood Map Modernization: Federal Emergency Management Agency's Implementation of a National Strategy (Testimony).** The Federal Emergency Management Agency (FEMA) is responsible for managing the National Flood Insurance Program (NFIP). The program uses flood maps to identify the areas at greatest risk of flooding and make insurance available to property owners to protect themselves from flood losses. According to FEMA, many of the nation's flood maps are more than 10 years old and no longer reflect current flood hazard risks because of erosion and changes in drainage patterns. Moreover, because many flood maps were created or last updated, there have been improvements in the techniques for assessing and displaying flood risks. This testimony is based on the Government Accountability Office’s findings and recommendations in its March 2004 report related to (1) how map modernization intended to improve the accuracy and accessibility of the nation's flood maps, (2) what the expected benefits of more accurate and accessible flood maps are, and (3) to what extent FEMA's strategy for managing the map modernization program support the achievement of these benefits.
Highlights: http://www.gao.gov/highlights/d05894thigh.pdf
Source: http://www.gao.gov/new.items/d05894t.pdf

[Return to top]

## Information Technology and Telecommunications Sector

**27.** *July 13, Security Focus* — **Mozilla Suite, Firefox and Thunderbird multiple vulnerabilities.** The Mozilla Foundation has released 12 security advisories specifying security vulnerabilities in Mozilla Suite, Firefox, and Thunderbird. These vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application, bypass security checks, execute script code in the context of targeted Websites to disclose confidential information; other attacks are also possible. These vulnerabilities have been addressed in Firefox version 1.0.5, Mozilla Suite 1.7.9. Mozilla Thunderbird has not been fixed at this time. The issues described here will be split into individual BIDs as further analysis is completed. This BID will then be retired.
Source: http://www.securityfocus.com/bid/14242/info

**28.**

*July 13, US−CERT* — **Technical Cyber Security Alert TA05−194A: Oracle Products Contain Multiple Vulnerabilities.** Oracle released a Critical Patch Update in July 2005 that addresses more than forty vulnerabilities in different Oracle products and components. The Critical Patch Update provides information about which components are affected, what access and authorization are required, and how data confidentiality, integrity, and availability may be impacted. Public reports describe vulnerabilities related to insecure password and temporary file handling and SQL injection. The impacts of these vulnerabilities vary depending on product or component and configuration. Potential consequences include remote execution of arbitrary code or commands, information disclosure, and denial of service. An attacker who compromises an Oracle database may be able to gain access to sensitive information. US−CERT strongly recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. Oracle HTTP Server is based on the Apache HTTP Server. Some Oracle products include Java components from Sun Microsystems. According to Oracle, the July 2005 Critical Patch Update addresses previously disclosed vulnerabilities in Apache and Java. Oracle also notes that Oracle Database Client−only installations are not affected by vulnerabilities listed in the July 2005 Critical Patch Update.
Oracle patch update: http://www.oracle.com/technology/deploy/security/pdf/cpujul2 005.html
Source: http://www.us−cert.gov/cas/techalerts/TA05−194A.html

**29.** *July 13, US−CERT* — **Vulnerabilities in MIT Kerberos 5.** Kerberos is a network authentication system which uses a trusted third party (a KDC) to authenticate clients and servers to each other. Several vulnerabilities have been reported. According to US−CERT Vulnerability Note VU#259798, an unauthenticated attacker can cause MIT krb5 Key Distribution Center (KDC) to overflow a heap buffer by one byte, possibly leading to arbitrary code execution. Patch details are available in MIT krb5 Security Advisory 2005−002. According to US−CERT Vulnerability Note VU#623332, an unauthenticated attacker can cause krb5_recvauth() function to free a block of memory twice, possibly leading to arbitrary code execution. Patch details are avilalbe in MIT krb5 Security Advisory 2005−003.
VU#259798: http://www.kb.cert.org/vuls/id/885830
MIT krb5 Security Advisory 2005−002:
http://web.mit.edu/kerberos/www/advisories/MITKRB5−SA−2005−0 02−kdc.txt
VU#623332: http://www.kb.cert.org/vuls/id/623332
MIT krb5 Security Advisory 2005−003:
http://web.mit.edu/kerberos/www/advisories/MITKRB5−SA−2005−0 03−recvauth.txt
Source: http://www.kb.cert.org/vuls/

**30.** *July 13, US−CERT* — **Multiple vulnerabilities in WebEOC.** The US−CERT has released serveral vulnerability notes to address issues in WebEOC is a web−based crisis information management application that provides functions to gather, coordinate, and disseminate information between emergency personnel and emergency operations centers (EOC). According to VU#258834, in numerous places in a WebEOC system, resources are requested via URIs. An attacker may be able exploit this design by crafting a URI that will directly access a resource, thus elevating that attacker's privileges. According to VU#491770, WebEOC uses weak algorithms to encrypt sensitive information. A remote attacker could recover or derive a private encryption keys, or apply simple cryptanalytic techniques to decipher an encrypted message. According to VU#138538, WebEOC contains multiple cross−site scripting

vulnerabilities. A remote attacker may be able to execute arbitrary script using a vulnerable WebEOC site. In addition, that attacker may be able to retrieve sensitive data from WebEOC site. According to VU#956762, WebEOC does not restrict the size of files that an authenticated user can upload into a back−end database. An authorized attacker may be able to consume a large amount of system resources. As system resources are exhausted, system operation may be disrupted resulting in a denial−of−service condition. According to VU#372797, a remote attacker may be able to execute SQL queries on a server, possibly with elevated privileges. As a result, attackers may be able to view or modify the contents of a WebEOC database. According to VU#165290, WebEOC insecurely stores sensitive information in easily accessible application components. Sensitive information may be easily accessible to untrusted parties.
VU#258834: http://www.kb.cert.org/vuls/id/258834
VU#491770: http://www.kb.cert.org/vuls/id/491770
VU#138538: http://www.kb.cert.org/vuls/id/138538
VU#956762: http://www.kb.cert.org/vuls/id/956762
VU#372797: http://www.kb.cert.org/vuls/id/372797
VU#165290: http://www.kb.cert.org/vuls/id/165290
Source: http://www.kb.cert.org/vuls/

**31.** *July 12, Cisco* — **Cisco CallManager memory handling vulnerabilities.** Cisco CallManager (CCM) is the software−based call−processing component of the Cisco IP telephony solution which extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice−over−IP (VoIP) gateways, and multimedia applications. Cisco CallManager 3.3 and earlier, 4.0, and 4.1 are vulnerable to Denial of Service (DoS) attacks, memory leaks, and memory corruption which may result in services being interrupted, servers rebooting, or arbitrary code being executed. Cisco has made free software available to address these vulnerabilities.
Source: http://www.cisco.com/warp/public/707/cisco−sa−20050712−ccm.s html

## 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 (−−−), 6881 (bittorrent), 445 (microsoft−ds), 27015 (halflife), 3800 (−−−), 139 (netbios−ssn), 80 (www), 135 (epmap), 32775 (sometimes−rpc13), 4672 (eMule)<br>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

**32.** *July 13, New York Times* — **Town uses trespass law to fight illegal immigrants.** One day last April, Jorge Mora Ramírez stopped his car on the side of a road in the small southern New Hampshire town of New Ipswich and was making a cell phone call when a police officer approached him. The officer questioned Ramírez, a 21−year−old Mexican who acknowledged that he was in the country illegally, and the New Ipswich police tried to get federal immigration authorities to arrest him. But when immigration officials demurred, not considering him a priority given scarce enforcement resources, the police acted on their own. They took the highly unusual step of charging Ramírez with criminal trespassing, and held him overnight. Other police departments, in states that include California, Florida and Georgia, have called New Ipswich police chief W. Garrett Chamberlain for advice. And immigration experts say that if the New Hampshire charges are upheld, some local law enforcement officials around the country will most likely copy the approach. The prosecutor, Nicole Morse, says that local police agencies had a right to cite illegal immigrants. "Indeed, the state's interest in this case is security. Being able to identify people who are in our community is essential to the police being able to maintain and keep the peace."
Source: http://www.nytimes.com/2005/07/13/national/13immigrants.html

[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.