Department of Homeland Security Daily Open Source Infrastructure Report for 27 August 2007

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

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

Daily Highlights

- The Department of Homeland Security's Domestic Nuclear Detection Office has announced the graduation of the first class of the Advanced Radiation Detection course, providing state, local, and municipal jurisdictions with skills to detect and investigate the potential malicious use of radioactive or nuclear material. (See item 3)
- The Federal Aviation Administration is testing an experimental, satellite−based navigation system called NextGen that hopefully can prevent gridlock in the skies in the coming decades. (See item 11)
- Attention DHS Daily Report readers:
  After five years, the production of the DHS Daily Report is transitioning to a new research team effective for the Tuesday, August 28, edition. The format of the DHS Daily Report will remain the same, but starting at the end of this week, it will be disseminated from a new email address: NICCREPORT@dhs.gov. Please stay tuned over the next few days for an announcement of the activation of the new email address and prepare to adjust your mail filters accordingly. Thank you for your support during this transition.

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) −

http://www.esisac.com]

1. *August 24, Reuters* — **Oil prices jump back over $70 a barrel on refinery woes.** Oil prices jumped more than at $1 to over $71 a barrel on Friday, August 24, as U.S. refinery problems spurred concerns about fuel supplies in the world's top consumer. U.S. crude for October delivery gained $1.42 to $71.24 a barrel, after a 57 cents gain on Thursday. London Brent crude rose 89 cents to $70.75 a barrel, after closing at a premium to U.S. oil on Thursday for the first time since July 27. A string of refinery outages during the U.S. summer gasoline season have helped support prices in recent months. Oil has also been sensitive to weakness in world stock markets caused by concerns over the impact of troubles in the U.S. mortgage market on the wider economy. The U.S. mortgage crisis has spread to other markets in recent weeks and oil has been hit as investors, fearing a credit squeeze, have sold to raise cash.
Source: http://www.usatoday.com/money/industries/energy/2007−08−24−o il−prices_N.htm

2. *August 24, Associated Press* — **Storms' effects knock out power to thousands.** It could take electric utilities days to restore power to all customers left in the dark by this week's storms, officials said. Power was restored by Saturday morning, August 25, to more than half a million customers in Illinois, but about 120,000 ComEd customers in northern Illinois remained without electricity, said ComEd spokesperson Joe Trost. In southern Michigan, more than 100,000 customers were without power Saturday, utilities said. Powerful storms a day earlier spawned at least one tornado that destroyed several homes and barns in Fenton, and minor injuries were reported.
Source: http://www.cnn.com/2007/US/08/25/severe.weather.ap/index.htm l

3. *August 24, Department of Homeland Security* — **DHS graduates first advanced radiation detection course.** The Department of Homeland Security's (DHS) Domestic Nuclear Detection Office (DNDO) announced on Friday, August 24, the graduation of the first class of the Advanced Radiation Detection (ARD) course in Las Vegas, NV. The five−day course focuses on the preventive radiological and nuclear detection (PRND) mission and provides participants from state, local, and municipal jurisdictions with the skills needed to detect and investigate the potential malicious use of radioactive or nuclear material. "The Advanced Radiation Detection course is the capstone course in the national preventive radiological and nuclear detection curriculum," said Vayl S. Oxford, DNDO director. "This curriculum aids state and local jurisdictions in joining the national radiological and nuclear detection mission." ARD course graduates learned skills in detecting radioactive material, assessing detection instrument alarms, and adjudicating radiological and nuclear alarms. DNDO oversees and executes the national PRND training and exercise policy, which offers federal, state, and local law enforcement and emergency responders the opportunity to enhance local PRND capabilities. DNDO is a jointly staffed office that was established in 2005 to improve and to further enhance the nation's capability to detect nuclear or radiological material that may be used against the homeland.
Source: http://www.dhs.gov/xnews/releases/pr_1187992420985.shtm

[Return to top]

Chemical Industry and Hazardous Materials Sector

4.

August 23, Arizona Republic — **Factory ammonia leak prompts road closures.** An ammonia leak from an ice factory near 19th Avenue and Peoria Avenue in Phoenix, AZ, Thursday afternoon, August 23, caused the factory to be evacuated and closed nearby roads. There were no serious injuries from the inhalation of the ammonia fumes, but two people from the building across from the factory who stepped outside shortly after the leak complained of shortness of breath and rash. High−pressure ammonia lines that run along the roof of the ice factory to chill the freezers sprung a leak and emitted concentrated amounts of ammonia. Although the concentrations of dangerous fumes were relatively low by Thursday evening, fire officials continued to recommend that people living or working nearby remain indoors. Roads were closed Thursday afternoon and evening from 21st Street to 15th Avenue and from Vogel Avenue to Cheryl Drive.
Source: http://www.azcentral.com/community/phoenix/articles/12n−HazmatSituation0823−CR−CP.html

[Return to top]

Defense Industrial Base Sector

5. *August 23, Federal Computer Week* — **Air Force seeks new ideas for support missions.** The Air Force is looking for technologies that could help improve the service's ability to conduct combat support operations, according to an August 21 Department of Defense notice published on the Federal Business Opportunities Website. The notice said the service's Agile Combat Support Modernization Analysis Working Group is seeking ideas from industry and academia to offset limitations on support operations Air Force officials anticipate between 2010 and 2035. These limitations include obstacles typically associated with military work in austere environments worldwide, potential force reductions and budget shortfalls, the notice said. The Air Force is particularly interested in ideas that would reduce the need for airlift in and out of future theaters, and technologies capable of cutting the number of personnel needed to initiate and support military operations.
Air Force solicitation:
http://www.fbo.gov/spg/USAF/AFMC/AAC/Reference−Number−ACSSS−07−08−01/listing.html
Source: http://www.fcw.com/article103574−08−23−07−Web

[Return to top]

Banking and Finance Sector

6. *August 24, Reuters* — **Monster.com took five days to disclose data theft.** Monster.com waited five days to tell its users about a security breach that resulted in the theft of confidential information from some 1.3 million job seekers, a company executive told Reuters on Thursday, August 23. Hackers broke into the U.S. online recruitment site's password−protected resume library using credentials that Monster Worldwide Inc. said were stolen from its clients, in one of the biggest Internet security breaches in recent memory. They launched the attack using two servers at a Web−hosting company in Ukraine and a group of personal computers that the hackers controlled after infecting them with a malicious software program known as

Infostealer.Monstres, said Patrick Manzo, vice president of compliance and fraud prevention for Monster, in a phone interview. The company first learned of the problem on August 17, when investigators with Internet security company Symantec Corp told Monster it was under attack, Manzo said. Manzo said that based on Monster's review, the information stolen was limited to names, addresses, phone numbers and e−mail addresses, and no other details including bank account numbers were uploaded.
Source: http://www.eweek.com/article2/0,1895,2174995,00.asp

7. *August 24, ComputerWorld* — **Monster.com data may have been looted weeks ago.** The phishing attacks and Trojan horse infections that rely on personal information stolen from Monster.com to dupe recipients have been going on for weeks, perhaps months, according to reports by security researchers. Although Symantec Corp. only announced on August 17 that it had found a hacker−controlled server containing contact information on 1.3 million Monster.com users, traces of that information can be found in messages trying to infect PCs with ransomware as early as the first week in July. In a July 19 posting on the blog of UK−based security company Prevx Ltd., Jacques Erasmus, the company's director of malware research, outlined a run of spoofed Monster.com messages that hyped a download of something called Monster Job Seeker Tool. Users who took that bait, however, actually ended up infecting their Windows PCs with a piece of ransomware that encrypted files and demanded $300 to unlock them. Like other messages traced to the data−thieving Infostealer.Monstres Trojan that Symantec said looted the Monster.com resume database, the message included the real names of Monster job seekers in its salutation.
Prevx Blog: http://www.prevx.com/blog/52/Connecting−the−dots−on−the−ransomware−case.html
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032638&source=rss_topic85

[Return to top]

Transportation and Border Security Sector

8. *August 24, Government Accountability Office* — **GAO−07−1001: Very Light Jets: Several Factors Could Influence Their Effect on the National Airspace System (Report).** For several years, a number of aviation manufacturers have been designing and testing very light jets, a type of small jet aircraft equipped with advanced technologies and priced below other business jets. Aviation forecasters predict that thousands of very light jets will enter the National Airspace System (NAS) over the next two decades, contributing to the overall growth of the general aviation fleet. In 2006, the Federal Aviation Administration (FAA) certified the first very light jets for flight. This report identifies (1) current very light jet forecasts and what factors could affect very light jet deliveries, (2) how increasing numbers of very light jets might affect the capacity and safety of the NAS, (3) how FAA is planning to accommodate the entry of very light jets into the NAS, and (4) how very light jets might affect FAA’s costs and Airport and Airway Trust Fund revenues. To address these issues, the Government Accountability Office (GAO) reviewed relevant documents and interviewed agency officials and aviation experts. GAO is not making recommendations in this report. The Department of Transportation provided technical clarifications, which were incorporated as appropriate.
Highlights: http://www.gao.gov/highlights/d071001high.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−1001

9. *August 24, CNN* — **Storms play havoc with travel in Midwest, Southeast.** Severe weather in the U.S. Midwest and Southeast bedeviled air traffic, knocked out power to large sections of Chicago and pushed rivers and streams out of their banks. Flood watches and warnings were posted Thursday night and Friday, August 24, for parts of Nebraska, Kansas, Iowa, Missouri, Illinois, Indiana, Wisconsin, Michigan, and Ohio. Thousands of passengers at Chicago's O'Hare International Airport were significantly delayed early Friday as 90 percent of departures were running late or very late overnight. More than 500 flights out of the city's two main airports were canceled Thursday due to severe weather, and more delays could be expected Friday as thunderstorms remained in the forecast.
Source: http://www.cnn.com/2007/US/08/24/severe.weather/index.html

10. *August 24, Baltimore Sun* — **Chunks of concrete fall from bridge over Route 295 in Maryland.** A portion of the Baltimore Washington Parkway in Prince Georges County, MD, has been closed after chunks of concrete fell from a bridge onto the roadway. Shortly after noon, concrete portions of the Greenbelt Road Bridge fell onto the northbound lanes of the parkway, according to the United States Park Police. Lanes in both directions had been closed, but the southbound lanes have been reopened to traffic. No crashes or injuries were reported, but northbound traffic is being diverted onto the Capital Beltway, Interstate 495. The parkway will remain closed until the bridge is inspected and declared safe, officials said. A spokesperson for the U.S. Park Police said that some of the pieces of fallen concrete.
Source: http://www.baltimoresun.com/news/traffic/bal−bridge0824,0,2346600.story?coll=bal_tab01_layout

11. *August 24, WUSA9 (DC)* — **FAA testing navigation system expected to reduce flight delays.** Nearly 6,000 feet above eastern Maryland, a small triangle pops up on the aircraft navigational system, showing another plane less than five miles away. An experimental, satellite−based navigation system shows it clearly on a brightly colored screen that provides a detailed picture of all the planes nearby. The small screen and its array of green crescent blips are part of a fledgling air traffic control system called NextGen that the Federal Aviation Administration (FAA) hopes can prevent gridlock in the skies in the coming decades. The agency hopes it can eventually help reduce flight delays by allowing aircraft to fly closer together in the crowded skies and enabling pilots to weave their own courses. The FAA is asking Congress to approve $4.6 billion over the next five years for developing the system, currently being tested on flights in Alaska. Manny Weiss, FAA's eastern regional administrator, said the country needs to get away from World War II−era navigational systems, which are in dire need of repairs and upgrades.
Source: http://www.wusa9.com/news/news_article.aspx?storyid=62140

12. *August 24, Department of Homeland Security* — **DHS and Arizona team up to advance Secure ID initiatives.** The Department of Homeland Security (DHS) and the state of Arizona agreed to partner on efforts that will potentially enhance the security of the state driver's license to meet Western Hemisphere Travel Initiative (WHTI) requirements, provide Arizona employers with a secure document that can be used in validating a person's legal status and align to satisfy future requirements of REAL ID. The Arizona project, much like the agreement reached with the states of Washington and Vermont earlier this year will serve as another

alternative available to U.S. citizens to satisfy WHTI requirements. DHS announced in June that U.S. and Canadian citizens will need to present either a WHTI compliant document or government−issued photo ID and proof of citizenship, such as a driver's license and birth certificate, beginning on January 31, 2008, for admissibility into the U.S. The state of Arizona will develop a technologically enhanced driver's license that will provide its residents, who voluntarily apply and qualify, with a document that is acceptable for use at U.S. land and sea ports. The enhanced driver's license will be slightly more expensive than a standard Arizona state driver's license and will require proof of citizenship, identity, and residence.
Source: http://www.dhs.gov/xnews/releases/pr_1187969723463.shtm

[Return to top]

Postal and Shipping Sector

13. *August 22, Memphis Business Journal* — **FedEx opens two facilities on Mexican border.** FedEx Corp. is expanding its cross−border distribution with two new facilities in El Paso, TX, and Ciudad Juarez, Mexico. Smoother flow of goods between the two countries, according to FedEx, will simplify cross−border trade and help businesses on both sides of the border flourish. "With this expanded cross−border solution, FedEx looks to simplify the supply chain process by managing the transportation, brokerage and distribution of shipments that cross the Mexico−U.S. border on a regular basis," said Ed Clark, CEO and president of FedEx Trade Networks, in a statement.
Source: http://biz.yahoo.com/bizj/070822/1509778.html?.v=1

[Return to top]

Agriculture Sector

14. *August 25, Reuters* — **France extends farm restrictions due blue tongue.** The French Agriculture Ministry said on Saturday, August 25, it had extended restrictions on livestock movements to 19 regions from 17 following the discovery of two new cases of blue tongue in animals near the German border. The ministry said it had now notified 54 cases of the disease to the European Commission and world animal health body. The Dutch agriculture ministry said on Wednesday, August 22, it had extended movement restrictions to the whole of the Netherlands after the virus spread outside the existing restriction zone. It said 336 farms were affected, up from 268 just two days earlier.
Source: http://www.reuters.com/article/environmentNews/idUSL25459322 20070825?feedType=RSS&feedName=environmentNews&rpc=22&sp=tru e

15. *August 24, Animal and Plant Health Inspection Service* — **USDA distributes oral rabies vaccine across Appalachian states.** The U.S. Department of Agriculture’s (USDA) Animal and Plant Health Inspection Service (APHIS) will distribute oral rabies vaccine baits beginning on or about August 23 to prevent the spread of raccoon rabies in portions of West Virginia and southwestern Pennsylvania. In cooperation with state departments of agriculture, health and key agencies, baits containing oral rabies vaccine will be distributed over rural areas using low−flying twin−engine aircraft. Hand baiting will occur in populated regions using

ground−based vehicles. The projected one−week program will target raccoons and distribute approximately 1.5 million baits covering roughly 9,500 total square miles in two states. Since 1997, APHIS has been working to establish a rabies−free barrier in the eastern U.S. where the raccoon variant of rabies threatens wildlife populations and pets, as well as public health and safety. APHIS has coordinated a cooperative effort in the following states: Alabama, Florida, Georgia, Maine, Maryland, Massachusetts, New Hampshire, New York, North Carolina, Ohio, Pennsylvania, Tennessee, Vermont, Virginia and West Virginia.
Source: http://www.aphis.usda.gov/newsroom/content/2007/08/rabieswvp a.shtml

16. *August 22, Denver Business Journal* — **Huge wheat harvest leads state to suspend trucking rules.** The largest wheat harvest in nearly a decade led Colorado Gov. Bill Ritter to declare a "disaster emergency." A shortage of commercial trucks to move the wheat off the farms to storage facilities and railroad loading docks led Ritter to issue an executive order that suspends restrictions for using "farm−plated" vehicles to transport the crop. The suspension will last for 45 days, the governor's office said in the announcement. Many of the trucking and rail carriers that have moved the crops from the farms have gone out of business in the last few years due to drought, low commodity prices and high fuel prices. And with railcars limited, transportation costs have "become prohibitive," the statement said. About 10 million bushels of wheat, valued at more than $60 million, is currently on the ground on farms around the state. It will degrade if not moved to grain elevators soon. And the wheat already in some elevators must be moved to market to make room for the corn harvest that starts in late September, the governor's office said.
Source: http://www.bizjournals.com/denver/stories/2007/08/20/daily34 .html

[Return to top]

Food Sector

17. *August 25, U.S. Food and Drug Administration* — **Dog food recalled.** The U.S. Food and Drug Administration (FDA) is alerting consumers that Mars Petcare, has recalled two dry dog food products because of the potential contamination with Salmonella Schwarzengrund. The Mars Petcare, based in Franklin, TN, is voluntarily recalling five−pound bags of Krasdale Gravy dry dog food sold in Connecticut, Massachusetts, New Jersey, New York, and Pennsylvania, and 50−pound bags of Red Flannel Large Breed Adult Formula dry food sold in Pennsylvania. The FDA conducted tests on 10 samples, representing seven product brands from the company. Each sample (same size and brand of product) consisted of 15 subsamples, for a total of 150 subsamples. Tests of the 150 subsamples revealed two positive samples; one from the Krasdale Gravy dry food and another from Red Flannel Large Breed Adult Formula dry food. Salmonella can potentially be transferred to people handling pet food. To date, there have been 64 cases of illness in humans related to Salmonella Schwarzengrund reported to the U.S. Centers for Disease Control and Prevention (CDC); however, none of the reported cases have been directly linked to the recalled product that was tested. The FDA is working with local and state officials, and with officials at the CDC in the investigation.
Source: http://www.fda.gov/bbs/topics/NEWS/2007/NEW01689.html

18. *August 24, San Jose Mercury News (CA)* — **Jamba warns of hepatitis A exposure.** Santa Clara, CA, health officials warned Thursday, August 23, that customers of the Jamba Juice on

the corner of Lincoln Avenue and Willow Street may have been exposed to hepatitis A and should see their doctor. One of the food handlers at the store contracted the virus and may have worked in the store earlier this month while she was still infectious. County health officials said the risk to the public is low, but they are recommending some customers either get a hepatitis A vaccine or an immune globulin shot. The company said it has disposed of all food products, thoroughly cleaned the store and brought in replacement workers until the store's employees are also treated. Hepatitis A is a liver disease that can affect anyone. The virus is transmitted from person to person if something contaminated by the infected stool is put in another's mouth. Source: http://www.mercurynews.com/valley/ci_6706326

19. *August 24, California Department of Public Health* — **California Department of Public Health warns consumers not to eat Barrilito and Miguelito candies.** After finding potentially harmful levels of lead in Barrilito and Miguelito Mexican candies, the California Department of Public Health on Wednesday, August 23, warned consumers not to eat them. Mark Horton, director of the public health agency, said tests on the candies imported from Mexico found levels of lead that could cause health problems. Barrilito and Miguelito candies are distributed by TJ Candy Corp. of Montebello, CA, which has initiated a voluntary recall of the products and is working with the health agency to remove them. The health agency also is working to identify other California distributors that might sell these products. Source: http://www.contracostatimes.com/ci_6695945

20. *August 24, McClatchy Newspapers* — **Agents raid pork plant.** Federal immigration officials conducted a raid Wednesday, August 22, the second this year, at Smithfield Foods' pork slaughterhouse in Bladen, NC. Twenty−eight people stand accused of entering the country illegally and committing identity theft, said Richard Rocha, a spokesperson for Immigration and Customs Enforcement. Twenty−five were from Mexico, two were from Guatemala and one from Honduras. Rocha said that the arrests were the result of an investigation and that the suspects were targeted, not part of a random sweep of illegal immigrants. Source: http://www.myrtlebeachonline.com/news/local/story/167433.htm l

21. *August 24, Hankyoreh (South Korea)* — **South Korea to resume U.S. beef imports.** South Korea announced, on Friday, August 24, the resumption of quarantine inspections of U.S. beef, which were halted after the detection of specific risk materials (SRM) in a shipment about 20 days ago. In addition, the government plans to start negotiations with the U.S. administration to revise South Korea's sanitary and phytosanitary regulations (SPS) prohibiting imports of bone−in beef. Until the two sides agree on a revised bill, South Korea will halt quarantine inspections for U.S. beef if risk materials are detected in future shipments. Source: http://english.hani.co.kr/arti/english_edition/e_business/23 1350.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

22. *August 26, Deutsche Welle (Germany)* — **Bird−flu find results in Germany's largest bird cull ever.** German health officials slaughtered 160,000 geese over the weekend after the H5N1 bird−flu virus was found in a poultry farm near the city of Erlangen on Friday, August 24. The cull was ordered after 400 geese were found dead. A team of eight vets and poultry workers at the farm in Wachenroth, Bavaria, started what officials called the biggest ever culling operation in Germany late on Saturday. Tests by the Friedrich Loeffler Institute of Veterinary Medicine had found the H5N1 strain of the virus in five of the birds.
Source: http://www.dw−world.de/dw/article/0,2144,2752566,00.html

23. *August 23, Associated Press* — **Bad tests led thousands to take whooping cough antibiotics needlessly.** A reported boom in U.S. whooping cough cases is now being questioned after health officials discovered a regularly used lab test misdiagnosed cases in suspected outbreaks in New Hampshire, Massachusetts and Tennessee. The false test results led thousands of people to take antibiotics unnecessarily and even caused a New Hampshire hospital to limit the number of patients admitted since hospital workers were thought to be infected. Pertussis, or whooping cough, is a potentially fatal bacterial respiratory infection. Government health officials say cases have tripled in the U.S. since 2001, with nearly 26,000 cases reported in 2005. Nearly half of those cases were diagnosed with the testing method now called into question, and that has raised doubts about the true number of cases. The most accurate diagnostic testing for whooping cough requires a week or more to grow the pertussis bacteria from a sample from a patient's nose or throat. Sometimes that is too long for health authorities to take action to prevent the disease from spreading. Increasingly, doctors have depended on a faster, but less accurate test. Different labs do the tests differently, leading to uneven results, experts say.
Source: http://www.iht.com/articles/ap/2007/08/23/america/NA−MED−US−Whooping−Cough.php

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24. *August 25, Associated Press* — **Officials in California show off new portable hospital.** State officials in California unveiled a 200−bed portable hospital Saturday, August 25, that can be deployed to the scene of a large−scale disaster. The hospital is one of three ordered by Governor Arnold Schwarzenegger. Officials displayed the new hospital at the Los Alamitos Joint Forces Training Base near Long Beach, where a weeklong training program for first responders and community volunteers will be hosted. The mobile hospitals can be moved in California Air National Guard airplanes. Each one can provide 23,000 square feet of hospital space and offers treatments ranging from emergency room services to surgery and intensive care.

Source: http://www.ksby.com/Global/story.asp?S=6983339

25. *August 25, Associated Press* — **Massachusetts governor to overhaul state's emergency response.** Two years after Hurricane Katrina highlighted woeful emergency planning, Massachusetts Governor Deval Patrick is poised to unveil a major overhaul to the state's response plan to a natural or manmade disaster. The Massachusetts State Police will be charged with overseeing the large−scale movement of traffic and the government will make plans for three large evacuation centers across the state. A task force will also oversee 10 conferences where agencies can coordinate dealing with vulnerable populations, such as the elderly, disabled and infirm. In addition, the governor plans to kick off a "Help Us Help You" awareness campaign next month that aims to preserve critical resources for first responders by encouraging the general public to develop personal and family emergency response plans. Source: http://www.boston.com/news/local/massachusetts/articles/2007/08/25/2_years_after_katrina_patrick_to_redo_mass_emergency_response/

26. *August 24, Federal Emergency Management Agency* — **President declares major disaster for Oklahoma.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Friday, August 24, that federal disaster aid has been made available for the state of Oklahoma to supplement state and local recovery efforts in the area struck by severe storms, tornadoes, and flooding beginning on August 18, 2007, and continuing. FEMA Administrator David Paulison said the assistance was authorized under a major disaster declaration issued for the state by President Bush. The President's action makes federal funding available to affected individuals in Blaine, Caddo and Kingfisher counties. Source: http://www.fema.gov/news/newsrelease.fema?id=39129

[Return to top]

Information Technology and Telecommunications Sector

27. *August 24, InformationWeek* — **Slammer worm still attacking.** Gunter Ollmann, director of security strategy at IBM's Internet Security Systems, said the most common malware attack today is coming from the Slammer worm, which hit in January of 2003. The worm is still working its way around the Internet and within corporate networks, according to Ollmann. And it's still spreading in a big way. And Slammer isn't the only piece of old−time malware that is still wreaking havoc. "The stuff [malware authors] wrote a while ago is still out there and still propagating and still infecting machines," he said. "Some have more infections now than they did when they were headline news. All those old vulnerabilities haven't all gone away." Slammer, the worm that brought many networks down to their knees by attacking Microsoft's SQL Server, is at the top of Ollmann's list of current malware problems. "When we hear about the latest worm and zero−day, Slammer still beats them by a long shot," he added. Source: http://www.informationweek.com/security/showArticle.jhtml;jsessionid=Z0QOZ5L1MAE1OQSNDLRSKHSCJUNN2JVN?articleID=20180226 6

28. *August 23, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA07−235A: Trend Micro ServerProtect Contains Multiple Vulnerabilities.** A number of vulnerabilities exist in the Trend Micro ServerProtect antivirus

product. These vulnerabilities could allow a remote attacker to completely compromise an affected system. Multiple buffer overflow vulnerabilities and an integer overflow vulnerability have been discovered in the RPC interfaces used by various components in Trend Micro's ServerProtect software package. These vulnerabilities could be exploited by a remote attacker with the ability to supply a specially crafted RPC request to the system running the affected software. Solution: Trend Micro has provided an update for these vulnerabilities in ServerProtect 5.58 for Windows NT/2000/2003 Security Patch 4 − Build 1185. Until the patch can be applied, administrators may wish to block access to the vulnerable software from outside their network perimeters, specifically by blocking access to the ports used by the ServerProtect service (5168/tcp) and the ServerProtect Agent service (3628/tcp). This will limit exposure to attacks; however, attackers within the network perimeter could still exploit the vulnerabilities. ServerProtect 5.58 for Windows NT/2000/2003 Security Patch 4 − Build 1185: http://www.trendmicro.com/ftp/documentation/readme/spnt_558_win_en_securitypatch4_readme.txt
Source: http://www.uscert.gov/cas/techalerts/TA07−235A.html

29. *August 23, eWeek* — **Hackers hit Trend Micro's ServerProtect.** Hackers have set their sights on security vendor Trend Micro's ServerProtect. Several security researchers have noted a massive increase of activity over TCP port 5168 connected with ServerProtect, an anti−virus software product for servers that had a number of vulnerabilities publicly disclosed earlier the week of August 20. All of the vulnerabilities, which could lead to remote code execution, have been patched and the security fixes are available to customers. "Various people are abuzz trying to figure out what malware is behind this," Jose Nazario, senior security researcher at Arbor Networks, in Lexington, MA, wrote on a company blog. "At present it seems to be a botnet causing all of the havoc." Officials at Symantec said in an alert Thursday, August 23, that they have observed active exploitation of a Trend Micro ServerProtect vulnerability affecting the ServerProtect service on a DeepSight honey pot and are checking to see what vulnerability had been targeted. The company advised administrators to block TCP port 5168 at the network boundary or deploy strict IP−based access control lists to hamper hacking attempts.
Source: http://www.eweek.com/article2/0,1895,2174804,00.asp

Internet Alert Dashboard

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information
Attention DHS Daily Report Readers: After five years, the production of the DHS Daily Report is transitioning to a new research team effective for the Tuesday, August 28, edition. The format of the DHS Daily Report will remain the same, but starting at the end of this week, it will be disseminated from a new email address: NICCREPORT@dhs.gov. Please stay tuned over the next few days for an announcement of the activation of the new email address and prepare to adjust your mail filters accordingly. Thank you for your support during this transition.

Content and Suggestions: Until further notice, please continue to send mail to dhsdailyadmin@mail.dhs.osis.gov.
Subscription and Distribution Information: Until further notice, please continue to send mail to dhsdailyadmin@mail.dhs.osis.gov.

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.