



Department of Homeland Security Daily Open Source Infrastructure Report for 08 August 2006

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- BP Exploration Alaska officials struggled Monday, August 7, to assess suspected pipeline corrosion that will shut shipments from the nation's biggest oilfield, removing about eight percent of daily U.S. crude production and driving oil prices sharply higher. (See item [1](#))
- NBC4 reports a problem with Federal Aviation Administration equipment used when aircraft pilots must make instrument landings has forced the closure of one of the two landing runways at Los Angeles International Airport. (See item [16](#))
- The Associated Press reports a London-to-Boston flight — American Airlines Flight 109, a Boeing 777 — was called back to Heathrow Airport on Monday, August 7, after U.S. authorities discovered a passenger's name was on their "no-fly" list. (See item [17](#))

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 07, Associated Press* — **BP shuts down largest U.S. oil field.** BP Exploration Alaska scrambled Monday, August 7, to assess suspected pipeline corrosion that will shut shipments from the nation's biggest oilfield, removing about eight percent of daily U.S. crude production and driving oil prices sharply higher. BP, which is already facing a criminal investigation over a

large spill in March at the same Prudhoe Bay oilfield, did not know how long the field would be offline. BP suspects corrosion in both damaged lines. Steve Marshall of BP Exploration Alaska said tests indicated that there were 16 anomalies in 12 areas in an oil transit line on the eastern side of Prudhoe Bay. Tests found losses in wall thickness of between 70 and 81 percent. Repair or replacement is required if there is more than an 80 percent loss. Workers also found a small spill of about four to five barrels. The shutdown comes at a worrisome time for the oil industry, with supply concerns stemming both from the hurricane season and instability in the Middle East. "Oil prices could increase by as much as \$10 per barrel given the current environment," said Tetsu Emori of Mitsui Bussan Futures.

Source: http://www.nytimes.com/aponline/business/AP-Oil-Field-Shutdown.html?_r=1&oref=slogin

2. *August 07, Associated Press* — **Department of Energy ready to tap emergency oil.** The Department of Energy (DOE) is prepared to provide oil from the government's emergency supplies if a refinery requests it because of the disruption of supplies from Alaska, said DOE spokesperson Craig Stevens, referring to the loss of nearly half of oil shipments from Alaska's North Slope because of a pipeline corrosion problem. Stevens said the department will be in contact with BP Exploration Alaska Inc. and West Coast refiners later in Monday to assess the situation. The Strategic Petroleum Reserve is the nation's emergency stockpile of crude oil. The reserve has about 700 million barrels in storage on the Gulf Coast to be used in case of a serious supply disruption. DOE has lent SPR oil to refineries when there were disruptions because of pipeline or other problems. Most of Alaska's oil goes to refineries on the West Coast. It was unclear how those refineries would be supplied with oil on the Gulf Coast. However any oil put into the market to replace lost Alaska oil would tend to ease prices, market experts say.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080700308.html>

3. *August 05, NY1 News (NY)* — **Con Ed says repairs to electric grid may take seven months.** In a report issued Friday, August 4, Con Edison says it could take until February to repair the damaged power system in Northwest Queens. The 69-page document submitted to state energy regulators says the company plans to have on average about three percent of its electric operations crew — about 100 workers — in the area through the beginning of next year, tending to the failed system. Con Ed is fixing what brought about last month's outage in an attempt to prevent a devastating repeat. This report is Con Ed's second attempt. The state commission that oversees the utility rejected the first one, calling it "unresponsive and virtually useless."

Source: <http://www.ny1.com/ny1/content/index.jsp?stid=10&aid=61584>

4. *August 04, Utility Automation & Engineering* — **New high temperature superconductivity cables installed in New York.** A system that eliminates the resistance that causes power losses in traditional copper cables has begun operating, providing enough power for more than 70,000 area households in Albany, NY. Between electric utility National Grid's Riverside and Menands substations in Albany and directly below Interstate 90, superconducting wire is wrapped to form 382 yards of cable. To achieve superconductivity, or zero resistance, the wire and cables are cooled inside a vacuum jacket containing liquid nitrogen, pumped and cooled continuously by a cryogenic system. One HTS cable is designed to deliver three to five times more power than a conventional cable, which means utilities can accommodate demand increases without

having to add multiple distribution lines. The HTS cable promises to eliminate losses and enable the power level to be maintained throughout the system. Project funding was provided by the New York State Energy Research and Development Authority and the U.S. Department of Energy.

Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICLE_ID=261642&p=22

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

- 5. August 07, *eWeek* — Chemical industry giants zone in on cyber security.** In a worst-case scenario, lax cyber security at a chemical company could be truly explosive. Security inadequacies have the potential to result in safety risks to plant employees and local communities, business interruption, lost capital, physical attack, identity theft for the purpose of acquiring chemicals, and access to systems to cause plant disruptions, according to a position paper issued by the Chemical Information Technology Council Executive Board. To help one another as well as other chemical industry players maximize cyber-security, industry leaders Dow Chemical, DuPont, Rohm and Haas, Eastman Chemical, Nova Chemicals, and Celanese are stepping up their efforts with the alliance they had previously formed -- the Chemical Sector Cyber Security Program (CSCSP). To achieve its goals, the CSCSP must partner with business, industry and vendors. That's why getting IT suppliers on board with the group is a key initiative in 2006. The CSCSP currently has identified 29 prospective IT service and product providers that it's targeting for affiliate membership.

Guidance for Addressing Cyber Security in the Chemical Sector:

http://www.chemicalcybersecurity.com/cybersecurity_tools/ProgramCyberSecurityGuidanceFINAL.pdf

CSCSP Website: <http://www.chemicalcybersecurity.com/>

Source: <http://www.eweek.com/article2/0%2C1895%2C1998047%2C00.asp>

- 6. August 07, *Marietta Daily Journal (GA)* — Explosives plant blast prompts evacuations.** Peach County, GA, authorities are investigating an early morning blast at an explosives plant near Byron that sent a 500-foot mushroom cloud into the air Monday, August 7. No one was hurt in the explosion at Pyrotechnic Specialties Inc., but dozens of families were evacuated from their homes for about half an hour. The blast was felt as far away as Macon, which is about 15 miles from the plant.

Source: <http://www.mdjonline.com/articles/2006/08/07/95/10227342.txt>

- 7. August 03, *News Channel 5 (TN)* — Chemical cloud in Tennessee prompts evacuations.** Wednesday night, August 2, a leak at the Palm Commodities plant in LaVergne, TN, sent a two-mile long cloud of gas into the air. Officials said a failed pump allowed ammonia and hydrochloric acid to mix together forming the cloud. The area was evacuated, but after several hours investigators determined the cloud was not toxic.

Source: <http://www.newschannel5.com/content/news/21167.asp>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[[Return to top](#)]

Banking and Finance Sector

- 8. *August 07, Finextra* — Matrix Bancorp reports computer theft.** Matrix Bancorp has become the latest U.S. financial institution to report the theft of computer equipment containing the confidential account details of banking customers. The bank is investigating the theft of two laptops from its headquarters in Denver, CO, on Friday, July 28. The computers were stolen from the branch in a daytime heist, between 1:30 pm and 2:30 pm MDT when office staff were "temporarily absent". One of the laptops contains what the bank calls "certain proprietary information regarding Matrix Capital Bank and some of its customers". Matrix says the stolen laptops are password protected and the information on them encrypted. The bank is contacting affected customers but says it has no reason to believe that any confidential data has been misused.

Source: <http://finextra.com/fullstory.asp?id=15688>

- 9. *August 07, Associated Press* — U.S. fights North Korea over fake currency.** For those who have handled them, North Korean "supernotes" are virtually indistinguishable from the \$100 bills they mimic -- near-perfect forgeries of the most widely circulated American bank note outside the U.S. In congressional testimony, court papers, and interviews, current and former U.S. officials have described what they say is an unprecedented effort by a reclusive, communist-led government to support itself with criminal activity, including counterfeit \$100 bills. The supernotes' trail begins in 1989, when the bills were detected in the Philippines, and stretches from Asia to Europe to both coasts of the U.S. The fakes, say David Asher, a former State Department official on North Korea, "have been detected essentially on every continent in the world in the last 15 years." North Korea denies the counterfeiting charges. But the Secret Service has seized about \$50 million worth of supernotes worldwide. Analysts say much more is likely in circulation. Still, the problem the supernotes pose for the U.S., officials say, is not the quantity but the high quality of the bills, which mimic the real thing right down to similar "reverse-engineered paper" and security features, such as special red and blue fibers, threads, and a watermark.

Source: http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080700046_pf.html

- 10. *August 06, IDG News Service* — Cybercriminals taking cues from Mafia, says FBI.** The Website offered to sell stolen credit card information for \$100, but it was the title of the poster that caught FBI agent Thomas X Grasso Jr.'s attention. The cybercriminal identified himself as a "Capo di capo" -- a boss of bosses, in Mafia parlance. As money has become the driving force behind online threats, cyber criminals have adopting the same kind of organizational structures as organized crime groups, Grasso said Friday, August 4, at the Defcon hacker conference. "This organized crime group, Carderplanet, organized themselves into the same structure as the Italian Mafia," said Grasso. The FBI estimates that cybercrime cost the U.S. more than \$67 billion last year, Grasso said. Grasso then played a slick promotional video

offering Carderplanet "business" services. It could easily have been mistaken for a legitimate IT consulting ad. Carderplanet is just one part of a larger confederation of online criminals called the International Carder's Alliance. They use known Websites and IRC (Internet Relay Chat) channels to coordinate their online attacks. Many other cybercrime groups, such as Mazafaka, Shadowcrew, and IAACA (the International Association for the Advancement of Criminal Activity), are affiliated with Carderplanet.

Source: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002230&taxonomyId=17>

11. August 04, Register (UK) — Thai police crack credit card wiretap scam. Tourists from Australia and New Zealand are among an estimated 48,000 victims of a highly-organized credit card fraud ring in Thailand. According to local reports, crooks intercepted credit card data between merchants and banks in Phuket, the popular Thai resort town. The scammers loaded this data onto MP3 players, which they sent to accomplices in neighboring Malaysia. Cloned credit cards were manufactured in Malaysia and sent back to Thailand, where they were used to fraudulently purchase goods and services. Last month Thai tourist police arrested Tossapol Chaowanawuth, 42, in Bangkok's Chatuchak district, on suspicion of involvement in the wiretapping scam. Chaowanawuth has reportedly confessed to working with four accomplices on the scam. Further arrests are anticipated. Thai police began investigating after Visa International reported a large number of credit card frauds involving counterfeit cards.

Source: http://www.channelregister.co.uk/2006/08/04/thai_wiretap_scam/

12. August 04, eWeek — Cyber-thieves steal \$700K via ATM hacking. Cyber-thieves who hacked into the ATM information of at least 800 retail customers in California and Oregon have stolen as much as \$700,000 from personal accounts during the last two months, according to police reports. People who used ATM cards to purchase items at Dollar Tree, a national retail chain, in Modesto and Carmichael, CA, and Ashland, OR, have turned in reports of unauthorized withdrawals in the computer-based scam. It is unclear how the thieves stole the information, or how many shoppers were victimized. Brady Mills of the U.S. Secret Service said that the agency is investigating the thefts and that the bureau has been on the case for about two months. Dollar Tree customers in Modesto began reporting unauthorized ATM withdrawals from their bank accounts on June 12, according to the Modesto Bee newspaper. Local police said that more than 600 accounts were drained of approximately \$500,000. On August 1, police in Ashland confirmed that at least 200 people lost more than a total \$200,000 due to unauthorized bank account withdrawals after shopping at Dollar Tree stores in the Rogue Valley region of Oregon.

Source: <http://www.eweek.com/article2/0,1895,1999367,00.asp>

13. August 04, Government Executive — Agencies push to meet IT security deadline. Federal information security officials are struggling to comply with the June 23 Office of Management and Budget (OMB) mandate requiring agencies to improve the security of personally identifiable information by Monday, August 7. The memorandum was in response to a recent rash of data breaches reported across the government. The memo established a 45-day deadline for implementing a security checklist for protecting remote information. It also contained four OMB recommendations, including encrypting data on remote computer devices that hold sensitive information and permitting remote access only with two factors of authentication. According to several CIOs, agency inspectors general have initiated a review of compliance

with the checklist, which is based on previously established National Institute of Standards and Technology requirements. A report is expected in late September.

Source: [http://www.govexec.com/story_page.cfm?articleid=34713&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=34713&dcn=to%20daysnews)

[\[Return to top\]](#)

Transportation and Border Security Sector

14. August 07, VNUNet — Biometric passports cracked. Biometric passports used by the UK, U.S. and other countries have been cloned by a German security consultant, raising further doubts over the technology. Lukas Grunwald, a consultant with DN-Systems, told a Defcon security conference in Las Vegas that the data, stored on RFID chips, could be copied on to blank chips which could then be used in fake passports. Grunwald says it took just two weeks to figure out how to clone the passport chip, and cost him \$200. He tested the attack on a new European Union German passport, but the method would work on any country's e-passport, since all of them will be adhering to the same standard. Although he can clone the tag, Grunwald says it's not possible, as far as he can tell, to change data on the chip, such as the name or birth date, without being detected. Although countries have talked about encrypting data that's stored on passport chips, this would require that a complicated infrastructure be built first, so currently the data is not encrypted.

Source: <http://www.vnunet.com/computing/news/2161836/kacers-crack-biometric>

15. August 07, Transportation Security Administration — Trace portal machines deployed to Midway International Airport. The Transportation Security Administration (TSA) announced on Monday, August 7, that it has deployed two explosives detection trace portals to the passenger security checkpoint at Chicago's Midway International Airport. The state-of-the-art machines further enhance TSA's ability to detect explosives at the checkpoint and have added customer service benefits. Passengers identified for additional screening will walk through the trace portal for explosives detection screening. As they enter the trace portal, they will be asked to stand still for a few seconds while several "bursts" of air are released, dislodging microscopic particles from passengers that are then collected and analyzed for traces of explosives. A computerized voice indicates when a passenger may exit the portal. Security officers will take necessary and appropriate steps to resolve any alarms.

Source: http://www.tsa.gov/press/releases/2006/press_release_08072006.shtm

16. August 07, NBC4 (CA) — LAX incoming flights delayed due to system failure. Some incoming flights were delayed Monday, August 7, Los Angeles International Airport (LAX) because of a problem with Federal Aviation Administration (FAA) equipment used when aircraft pilots must make instrument landings, authorities said. The equipment failure, which forced the closure of one of the two landing runways at LAX, developed at about 9:30 a.m. PDT, said Tom Winfrey of Los Angeles World Airports. Tony Vella of the National Air Traffic Controllers Association said it was not clear how long it would take to repair the system. Allen Kenitzer of the FAA in Washington state said the failure of a "localizer" forced the closure of runway 25-Right. He said an interim solution was to reverse the landing pattern at LAX, with planes arriving from the west, instead of the normal pattern of flying in from the east. Vella said it was unknown what caused the equipment failure. Source:

Source: <http://www.nbc4.tv/travel/getaways/9640787/detail.html>

17. *August 07, Associated Press* — **Alert aborts London–Boston flight.** A London–to–Boston flight was called back to Heathrow Airport on Monday, August 7, after U.S. authorities discovered a passenger's name was on their "no-fly" list, officials said. American Airlines Flight 109, a Boeing 777, left London at 10:55 a.m. (5:55 a.m. EDT) headed for Boston, said Tim Wagner, a spokesperson for the Fort Worth, TX–based airline. "The flight returned to Heathrow due to a security issue that needed to be resolved in London," he said. "It was not a security threat to the aircraft. The flight was in no danger." Phil Orlandella, a spokesperson for the Massachusetts Port Authority, which runs Boston's Logan Airport, said staff were told at a meeting Monday morning that the name of a passenger on the flight matched one on the no-fly list. He had no further information. London's Metropolitan Police said port and border control officials were questioning four passengers removed from the flight.
Source: <http://www.cnn.com/2006/WORLD/europe/08/07/britain.plane.ap/index.html>
18. *August 07, WCAX (VT)* — **Train traffic brought to a halt in New York.** Work to clean up Sunday, August 6's train derailment in Moriah, NY, continues. Police say a Canadian Pacific train was traveling from Saratoga to Montreal, when 12 cars went off the tracks. The train was not carrying any hazardous materials. Several miles of tracks were damaged, and that has brought rail traffic to a halt. Crews hope to clean up the mess late Monday, August 7. Amtrak canceled its Albany to Montreal route on Monday, but hopes to resume service by Wednesday, August 9.
Source: <http://www.wcax.com/Global/story.asp?S=5246946>
19. *August 06, USA TODAY* — **Safety a concern as drones increase.** About 700 unmanned aerial vehicles (UAVs) operate in the U.S. Federal agencies such as the Coast Guard, NASA, Homeland Security, and the National Oceanic & Atmospheric Administration have expressed interest in using drones for everything from border surveillance to finding lost children. While most drones are small and fly only above military bases, some large UAVs are allowed under U.S. regulations to enter civilian airspace. President Bush has called for expanding their use to protect the nation's borders, and a handful of local police and sheriff's offices are seeking permission to use the planes, according to the Federal Aviation Administration (FAA). The airline pilots' union and the Aircraft Owners and Pilots Association (AOPA) say UAVs are not safe. "We are sharing airspace where we are assured that a certain level of safety is being met, and yet there is no level of safety for these UAVs," said Heidi Williams, air traffic services director for AOPA. The FAA has created a UAV division and is studying how to draw up standards for drones.
Source: http://www.usatoday.com/tech/news/surveillance/2006-08-06-drones_x.htm
20. *August 04, Government Accountability Office* — **GAO–06–1051R: Transportation Security Administration's Office of Intelligence: Responses to Posthearing Questions Regarding Secure Flight (Correspondence).** Enclosed are Government Accountability Office (GAO) responses to the supplemental questions submitted by the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment Committee on Homeland Security, House of Representatives. GAO's responses are based largely on information contained in the report entitled Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed (GAO–05–356, March 28, 2005), and testimonies entitled Aviation Security: Significant Management Challenges May Adversely

Affect Implementation of the Transportation Security Administration's Secure Flight Program (GAO-06-374T, February 9, 2006), and Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program (GAO-06-864T, June 14, 2006). As discussed in statements for over three years, the Transportation Security Administration (TSA) has faced numerous challenges in developing a federal passenger pre-screening program, known currently as Secure Flight, because TSA did not follow a disciplined life cycle development approach. Although TSA made some progress, it suspended the program's development earlier this year to reassess program direction, and it anticipates completing the reassessment by the end of September 2006.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-1051R>

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

Nothing to report.

[\[Return to top\]](#)

Food Sector

21. *August 07, Associated Press* — Shipment of U.S. beef arrives in Japan. Japan imported its first shipment of American beef since January on Monday, August 7, resuming a once-booming business that has been crippled for nearly three years over fears of mad cow disease. The 5.1 tons of American chilled beef arrived on a cargo flight at Tokyo's Narita airport, and its importer and government officials were expected to inspect it on Tuesday, August 8, said Health Ministry official Masanori Imagawa. Japan banned American beef in December 2003 after the first case of mad cow disease in the U.S. That ban was eased in December 2005, but was re-imposed after forbidden spine bones were found in an import shipment of veal in January. Monday's shipment follows the latest lifting of the beef ban on July 27.

Source: http://www.nytimes.com/aponline/business/AP-Japan-US-Beef.html?_r=1&oref=slogin

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

22. *August 07, Reuters* — **Thailand kicks off campaign to halt bird flu.** Thailand began a week-long campaign on Monday, August 7, to check every house in 29 provinces, including Bangkok's suburbs, in a bid to halt a resurging bird flu virus that has killed two people in the last three weeks. Hundreds of thousands of volunteers will scour backyard farms for sick or dead chickens and educate villagers on the H5N1 virus, which re-emerged in July after an eight-month lull. If any suspicious bird deaths are found, all poultry within a one mile radius of the suspected outbreak would be culled immediately. More than one third of Thailand's 76 provinces have been declared bird flu risk zones, but livestock officials said they had confirmed H5N1 in poultry in only two provinces, Pichit in the north and Nakhon Phanom in the northeast. However, health officials say a 27-year-old man who died in the central province of Uthai Thani, the country's second victim in two weeks, had caught the virus while burying sick chickens without wearing protective clothing.
Source: http://today.reuters.co.uk/news/articlenews.aspx?type=scienc eNews&storyID=2006-08-07T072517Z_01_BKK295755_RTRIDST_0_SCIE NCE-BIRDFLU-THAILAND-DC.XML
23. *August 07, Associated Press* — **Local tests indicate Indonesian boy has bird flu.** A 16-year-old Indonesia boy has tested positive for bird flu, health officials said Monday, August 7, citing local laboratory results that would take the total number of human infections in the country to 55. Additional tests were needed to confirm the results, but preliminary findings showed that the boy contracted the potentially fatal illness from sick chickens in Bekasi, east of the capital, Jakarta.
Source: http://www.thejakartapost.com/detailgen.asp?fileid=20060807_130052&irec=1
24. *August 06, Los Angeles Times* — **Tuberculosis diagnosis sometimes delayed by unfamiliarity in the U.S.** California businessman David Glasberg went to the top Los Angeles hospitals and even the Mayo Clinic in Minnesota for help. But his symptoms only worsened. No one guessed what it was until 11 years after he fell ill, when a doctor tried putting him on tuberculosis (TB) medications. He felt better in three weeks. Experts say cases such as Glasberg's are symptoms of a growing concern: Many doctors in the U.S. no longer recognize TB. Though relatively rare in the U.S., tuberculosis remains among the most common infectious diseases in the world, having killed 1.7 million in 2004. And it remains a danger in the U.S., especially in states such as California, with large numbers of immigrants from countries where the disease is endemic. Tuberculosis bacteria can remain dormant for years, then begin multiplying, particularly if the host's immune system is weakened. The disease still is generally treatable if caught early. But if diagnosis is delayed, it can permanently harm or kill its victims and spread to others.
TB information: <http://www.cdc.gov/nchstp/tb/default.htm>
Source: <http://www.latimes.com/news/printedition/front/la-me-tb6aug06.1.5901999.story?coll=la-headlines-frontpage&track=crosspro mo>
25. *August 04, University of Pennsylvania School of Medicine* — **Researchers determine structure of smallpox virus protein bound to DNA.** Researchers at the University of Pennsylvania School of Medicine have determined the structure of an important smallpox virus enzyme and how it binds to DNA. The enzyme, called a topoisomerase, is an important drug

target for coming up with new ways to fight smallpox. “This enzyme is one of the most closely studied DNA–modifying enzymes in biology,” says Frederic Bushman, Professor of Microbiology. “The structure of the DNA complex has been long–awaited.” DNA–modifying enzymes bind to specific sequences in the genetic code to aid in the many steps of DNA replication.

Source: http://www.uphs.upenn.edu/news/News_Releases/aug06/smlpxenz.htm

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

26. *August 07, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: For the North Atlantic, Caribbean Sea and the Gulf of Mexico shower activity associated with the remnants of tropical depression Chris has diminished and redevelopment is not expected. Western Pacific: Typhoon Saomai, upgraded from a Tropical Storm since leaving Guam and the Mariana Islands, continues moving northwestward, at 17 mph, 500 miles away from the Marianas, with maximum sustained winds of 75 mph. No U.S. interests are affected. Wildfire Update: Fire activity remains light throughout the nation with 133 new fires reported. To view other Situation Updates: <http://www.fema.gov/emergency/reports/index.shtm>
Source: <http://www.fema.gov/emergency/reports/2006/nat080706.shtm>

27. *August 07, Federal Computer Week* — **Researchers hope GPS data can shorten the time between tsunami detection and safety warnings.** A new tsunami–detection technique that uses Global Positioning System (GPS) data could potentially save many lives by helping alert people in time to escape. University researchers have shown that the technique, which relies on NASA–funded GPS software, can determine within 15 minutes whether an earthquake is strong enough to generate a tsunami like the one that devastated many parts of Asia in December 2004. The new approach, called GPS displacement, works by measuring the time it takes for radio signals from GPS satellites to arrive at ground stations close to the earthquake. Using that information, scientists can calculate how far the earthquake pushed the ground station. They enter that distance into a computer model that calculates the earthquake’s magnitude, which can then indicate whether a tsunami might occur. GPS–based detection offers the most advantages when an earthquake has a magnitude of at least 8.5, NASA scientists say. With the current detection methods, scientists struggle to rapidly assess the size of large earthquakes.
Source: <http://www.fcw.com/article95526-08-07-06-Print>

28. *August 06, Honolulu Star Bulletin* — **Hawaii to simulate nuclear terror attack.** For 34 straight hours beginning Tuesday, August 15, Hawaii’s Civil Defense planners will be manning the command center inside Diamond Head Crater in an exercise to cope with the effects of the detonation of a low–yield nuclear bomb planted by terrorists. The mock half–kiloton nuclear

explosion would take place at the entrance of Honolulu Harbor. But because it will take place near government centers of the state Capitol and City Hall, "the electromagnetic pulse could knock down 30 percent of our communications ability," said Edward Teixeira, state vice civil defense director. Teixeira said the drill is relevant because such communication loss could occur during any natural disaster like a hurricane and "it is something the state must constantly be ready to remedy." Coordinating the combined state–county–federal operation will be Maj. Gen. Vern Miyagi, who is the mobilization assistant to Adm. William Fallon, head of Pacific Forces in the Pacific. More than 700 state, city and military planners will participate in the mock exercise, dubbed "Exercise A Kele," running August 15–17.

Source: <http://starbulletin.com/2006/08/06/news/story09.html>

29. *August 05, Times–Picayune (LA)* — **Department of Homeland Security to help Louisiana with shelter shortage.** The nation's top homeland security official told Louisiana Governor Kathleen Blanco on Friday, August 4, that the federal government will help expand shelters in Louisiana for evacuees who don't have any other place to go when a hurricane threatens coastal parishes. Federal and state planning efforts have pegged the need for 150,000 shelter beds in Louisiana to deal with a Category 4 or 5 hurricane, according to a three–page letter signed by Department of Homeland Security Secretary Michael Chertoff. With the state able to support 65,000 spaces, the federal government will help in getting personnel and supplies for the remainder, he wrote. As the state heads into the heart of the Gulf Coast storm season in August and September, providing shelter space is one of the most critical components of being prepared for the next mass evacuation. Despite the offer of federal staffing help -- which Blanco has emphasized would be necessary to expand in–state shelter capacity -- the letter does not clear up all issues concerning how many shelters will be open this hurricane season.

Source: <http://www.nola.com/news/t-p/capital/index.ssf?/base/news-4/115475775598060.xml&coll=1>

30. *August 04, Federal Emergency Management Agency* — **President declares major disaster for Alaska.** The head of the Department of Homeland Security's Federal Emergency Management Agency on Friday, August 4, announced that Federal disaster aid has been made available for Alaska to supplement State and local recovery efforts in the area struck by snow melt and ice jam flooding during the period of May 13–30, 2006.

For further detail: <http://www.fema.gov/news/event.fema?id=6745>

Source: <http://www.fema.gov/news/newsrelease.fema?id=28588>

[[Return to top](#)]

Information Technology and Telecommunications Sector

31. *August 04, Government Computer News* — **The battle lines are drawn in the war on spyware.** The good news from the war on spyware is that there seems to be less support for organizations engaging in questionable behavior such as installing adware on the computers of unsuspecting users. But the bad news is that as the gray hats are being weeded out of the industry, the real bad guys are being left with the field to themselves. "We're seeing a lot more cases of keystroke loggers," said Ari Schwartz, deputy director of the Center for Democracy and Technology, during last week's Black Hat Briefings in Las Vegas. Although the application of criminal law has put a damper on the adware industry, what remains are those who are using

tools like keyloggers to steal passwords, account information and other valuable data. These threats are not likely to disappear soon.

Source: http://www.gcn.com/online/vol1_no1/41559-1.html?topic=security

32. August 04, *Government Computer News* — Senate ratifies international cybercrime treaty.

The Senate has ratified the Council of Europe Convention on Cyber Crime, the first multinational, multilateral treaty to require cooperation among law enforcement agencies in the investigation and prosecution of computer network crimes. The treaty has more than 40 signatory nations. "In particular, it will enhance our ability to cooperate with foreign governments in fighting terrorism, computer hacking, money laundering and child pornography, among other crimes," said Senate Foreign Relations Committee chairman Richard Lugar (R-IN).

Source: http://www.gcn.com/online/vol1_no1/41579-1.html?topic=security

33. August 04, *Information Week* — Vista vulnerable to stealthy malware. Under the right conditions, it's possible for a cyberattacker to inject arbitrary code into the Vista x64 kernel and stealthily take control of a user's system, according to one security researcher who demonstrated the process Thursday, August 3, at the Black Hat conference in Las Vegas. Joanna Rutkowska, a senior security researcher with Coseinc, presented a demo that showed how an attacker with systems administrator-level privileges could trick Windows Vista Beta 2 kernel, x64 edition, into disabling its signature-checking function and allow any unsigned device driver to be loaded onto a user's system. The danger is that the attacker can write malicious code into such a driver, which Vista would then execute.

Source: <http://www.informationweek.com/news/showArticle.jhtml;jsessionid=MKTXOX4VLSLA2QSNLQSKH0CJUNN2JVN?articleID=191800426>

34. August 04, *IDG News Service* — Mobile worm variant causes alarm. A security vendor has detected a new variant of an aggressive Russian mobile worm that uses some alarming new tricks. Like its earlier relatives, Commwarrior.Q will jump onto another phone using a short-range Bluetooth wireless connection, said F-Secure Corp. It also spreads via multimedia messaging service (MMS) or by an infected memory card inserted into a device.

Commwarrior.Q will continuously send MMS messages from midnight to 7 a.m. to people in an infected phone's address book. It cleverly assembles a text message from the phone's "sent" file, making it appear legitimate. After 7 a.m., however, Commwarrior.Q stops that action, as it would be noticeable to the user. It then starts scanning other phones to infect via Bluetooth.

F-Secure Advisory: http://www.f-secure.com/v-descs/commwarrior_q.shtml

Source: http://www.infoworld.com/article/06/08/04/HNmobiworm_1.html

35. August 04, *IDG News Service* — New Google feature flags dangerous sites. Google has begun alerting users whenever they click on a search result that may take them to a dangerous Website. The new feature, which had been spotted earlier last week, went live officially Friday, August 4, according to an announcement from The Stop Badware Coalition, which is collaborating with Google on this effort. When users attempt to click over to a Website considered to be potentially dangerous, Google shows users an alert page that informs them of the possible risk and gives them the option to click back to the results page or continue on to the questionable Website.

Source: http://www.infoworld.com/article/06/08/04/HNgoogleflags_1.html

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	1026 (win-rpc), 4672 (eMule), 445 (microsoft-ds), 32790 (----), 80 (www), 25 (smtp), 113 (auth), 6346 (gnutella-svc), 135 (epmap), 5900 (vnc) 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

36. August 07, Associated Press — First wave of New Orleans schools open. Eight New Orleans public schools reopened Monday, August 7, giving more than 4,000 students an early start on the school year and advancing a reform movement that blossomed after Hurricane Katrina devastated the city almost a year ago. More than 40 other public schools are scheduled to open by mid-September for an estimated 30,000 students in what is planned as a rebirth of one of the nation's worst school systems, which had about 60,000 students before the storm. Potential glitches remain. On Friday, August 4, for instance, state officials announced that one school wouldn't meet its target opening date of September 7 because of flooding during recent rains. Opening dates for several other schools are in question and state officials have acknowledged difficulties in finding enough teachers. A handful of schools remain under the authority of the troubled Orleans Parish School Board. The board has voluntarily allowed some schools to be run as "charter schools," which receive public money but operate independently. And it has been relieved of authority over more than 100 schools by the state Department of Education, which is running some of them itself and chartering others.

Source: http://www.usatoday.com/news/nation/2006-08-07-new-orleans-schools_x.htm

[[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

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.