



Department of Homeland Security Daily Open Source Infrastructure Report for 24 April 2007

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

- The Transportation Security Administration, American Association of Airport Executives, Airports Council International—North America, and National Air Transportation Association have announced a six–point plan to maximize the effectiveness of screening employees at airports. (See item [16](#))
- The General Services Administration has unveiled a redesign of USA.gov, the federal government’s official Web portal, which provides a centralized place to search for information on hundreds of government services, from checking tax refund status to contacting elected officials. (See item [27](#))

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. *April 23, WFAA-TV (TX)* — **Fire in the sky over East Fort Worth, Texas.** A huge fireball erupted Monday morning, April 23, near a power plant in East Fort Worth, TX. The fire spewed hundreds of feet from a large vertical pipe and could be seen for miles around, rocking an area near the Handley Steam Electric Station, a former TXU power plant now owned by Exelon Generation. The fire itself was at an Energy Transfers natural gas pipeline facility and burned intensely for about 30 minutes—at times resembling a fiery mushroom cloud. Fort

Worth Fire Department Lt. Kent Worley said the flare happened along a 24–inch transmission line that feeds the power plant. Worley said a relief valve tripped as designed, but a spark apparently ignited the volatile gas. Worley said there were no injuries. A worker at the facility on East Rosedale Street at South Handley Drive was able to shut off the valve, killing the flare. The source of the spark remained under investigation. The plant, which provides supplemental power during times of peak demand, was not on–line at the time of the fire.

Source: http://www.txcn.com/sharedcontent/dws/news/localnews/tv/stories/wfaa070423_wz_fwfire.38ced3ea.html

2. *April 21, Waxahachie Daily Light (TX)* — **Incidents at gas plant prompt evacuation, road closure.** A series of incidents at the Maypearl station of Enterprise Products Operating L.P. prompted authorities to close down a section of Farm–to–Market 916 twice Saturday, April 21, and evacuate residences within one half–mile of the plant, located at the corner of FM 916 and Brigman Road, west of the city. Emergency personnel first responded to a fire at the plant, which contains a large amount of natural gas and is located on a gas pipeline. The Maypearl Fire Department focused on isolating the incident and evacuating all structures within one half–mile of the plant. Gas company employees were able to close off a valve, and a decision was made to let the fire burn itself out. The fire completely involved one structure at the plant, and both Atmos Energy and Energy Transfer have operations at the plant. Before the fire burnt itself out, a pop–off valve blew, releasing a column of natural gas into the atmosphere and sounding “like a dozen jet engines,” according to one witness. No injuries relating to the fire were reported.

Source: <http://www.waxahachiedailylight.com/articles/2007/04/21/dailylight/news/00-04-20-gasplant.txt>

3. *April 21, Orlando Sentinel (FL)* — **Series of thefts hits utility.** Police are investigating several burglaries this month at the Progress Energy facility on Citrus Tower Boulevard in Clermont, FL. About 100 pounds of copper wiring were stolen, and the property and service vehicles have been burglarized four times since April 5. Progress Energy employees reported at least \$500 of damage. Authorities say the thieves cut through barbed wire and bent fencing to get in at night. Security cameras captured three men in the first burglary. Investigators also say this is when aluminum pieces were cut off a spool recovered about 40 feet from the fence.

Source: http://www.orlandosentinel.com/news/local/lake/orl-lbriefs21_607apr21.0.1270632.story?coll=orl-news-headlines-lake

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

Chemical Industry and Hazardous Materials Sector

4. *April 22, KRCG (MO)* — **Ammonia leak prompts road closure.** Residents in Chamois, MO, had a rude awakening early Sunday morning, April 22, when an ammonia leak filled the city with noxious chemicals. The Osage County Sheriff’s office along with Hazmat crews shut down the main roads into Chamois as they worked to contain the industrial grade ammonia leak at the MFA plant. Some residents are calling for more security at the plant. KRCG looked into records and found out that there have been previous leaks resulting in evacuations after attempts to steal ammonia from the tanks.

Source: http://www.krcg.com/news/news_story.aspx?id=33212

5. *April 22, CBS2Chicago* — **Ammonia leak prompts shut down.** An area cordoned off because of an ammonia leak in Bolingbrook, IL, was re-opened Saturday night, April 21. A quarter-mile surrounding the effected area was temporarily shut down, but has been opened to vehicles and pedestrian traffic. One tank of anhydrous ammonia had been on its side and another was leaking near the vicinity of West 111th Street and Kings Road. Each tank contained 1,000 pounds of ammonia.

Source: http://cbs2chicago.com/topstories/local_story_111215929.html

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

Defense Industrial Base Sector

6. *April 23, Government Accountability Office* — **GAO-07-525T: Stabilizing and Rebuilding Iraq: Conditions in Iraq Are Conducive to Fraud, Waste, and Abuse (Testimony).** Since 2003, the Department of Defense (DoD) has reported total costs of about \$257.5 billion for military operations in Iraq; these have increased from about \$38.8 billion in fiscal year 2003 to about \$83.4 billion in fiscal year 2006. The largest increase has been in operation and maintenance expenses, including items such as support for housing, food, and services; the repair of equipment; and transportation of people, supplies and equipment. Many of the operation and maintenance expenses are for services. Other U.S. government agencies had reported obligations of \$29 billion for Iraqi reconstruction and stabilization, as of October 2006. These funds have been used for, among other things, infrastructure repair of the electricity, oil, water, and health sectors; training and equipping of the Iraqi security forces; and administrative expenses. Comptroller General of the United States David M. Walker's testimony before the Subcommittee on Defense, House Committee on Appropriations focused on (1) security, (2) management and reporting of the program to train and equip Iraqi security forces, (3) contracting and contract management activities, and (4) Iraqi capacity and commitment to manage and fund reconstruction and security efforts.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-525T>

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

Banking and Finance Sector

7. *April 23, Reuters* — **Bank of America to buy LaSalle for \$21 billion.** Bank of America Corp. agreed to pay \$21 billion for ABN Amro Holding NV's LaSalle Bank Corp. unit, filling a big hole in its nationwide branch network by becoming Chicago's largest bank, and also becoming the biggest bank in slower-growing Michigan. The all-cash purchase will give Bank of America, the second-largest U.S. bank, 141 new branches in the Chicago area, 264 in Michigan and six in Indiana, as well as about 1,500 automated teller machines and about \$113 billion of assets. The purchase could bump Bank of America up against a federal cap that bars it from making acquisitions that would give it more than 10 percent of all U.S. deposits. Bank of America recently controlled just over nine percent. Chicago has experienced a surge in bank branches, so much so that Washington Mutual Inc., the largest U.S. savings and loan, is closing some branches there. Bank of America expects the LaSalle transaction to close in late 2007 or

early 2008.

Source: http://money.cnn.com/2007/04/23/news/companies/bank_of_america_lasalle.reut/?postversion=2007042309

8. *April 23, Associated Press* — **ABN Amro agrees to be bought by Barclays for \$91 billion.** Barclays PLC said Monday, April 23, it will acquire ABN Amro NV for \$91.16 billion in the world's largest bank takeover, capping a month of negotiations to create the global financial services giant. As part of the deal, ABN announced it is selling its U.S. unit LaSalle Bank to Bank of America Corp. for \$21 billion in cash. The proposed chief executive of the new group, Barclays CEO John Varley, called the deal “the largest merger ever in global financial industry,” and said it holds out the promise of growth at a rate twice as fast as global GDP. The companies said the deal would create a single bank, based in Amsterdam, with 47 million customers worldwide. Bank branches were likely to retain their brand names.
Source: <http://www.signonsandiego.com/news/business/20070423-0235-abnamro-barclays.html>

9. *April 23, Websense Security Labs* — **Phishing Alert: Commercial Bank of Kuwait.** Websense Security Labs have received reports of a phishing attack that targets Commercial Bank of Kuwait customers. Users receive a spoofed email message that claims a number of attempts were made to login to the user's account from a foreign IP address. The email states that the account was temporarily suspended pending re-activation, in order to protect the user. The email provides a link to a phishing site which attempts to collect personal and account information.
Source: <http://www.websense.com/securitylabs/alerts/>

10. *April 21, Associated Press* — **Paris anti-terrorism office investigates explosion at Marseille bank.** The Paris prosecutor's anti-terrorism office has taken over the investigation of an explosion that ripped through a Marseille bank, judicial officials said Saturday, April 22. No one was hurt Friday evening's explosion in a branch of the Caisse d'Epargne bank in the center of the Mediterranean port city. There have been no claims of responsibility for the blast, but the prosecutors office has said it appeared to be a terrorist attack, rather than a criminal one. Investigators were working under the theory that Corsican separatists were behind the incident, a police official said.
Source: <http://www.iht.com/articles/ap/2007/04/21/europe/EU-GEN-France-Marseille-Blast.php>

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

Transportation and Border Security Sector

11. *April 23, Reuters* — **Delta narrows loss as bankruptcy exit nears.** Bankrupt Delta Air Lines Inc., which expects to exit Chapter 11 within days, posted a narrower first-quarter loss on Monday, April 23, on higher fares and lower costs. The No. 3 U.S. airline, which aims to emerge from bankruptcy by the end of this month and list new shares in early May, reported a loss of \$130 million compared with a loss of \$2.1 billion in the year-ago quarter. Results in both periods were burdened by restructuring expenses. Excluding costs related to the carrier's

reorganization and other special items, Delta said it lost \$6 million, compared with a loss of \$356 million in the first quarter of 2006. Delta is exiting bankruptcy amid signs of softening demand for domestic U.S. air travel. A slowdown in air travel could threaten the long-suffering industry's nascent recovery. Once it emerges from bankruptcy, which could be set for April 30, Delta plans to cancel its current shares and issue new shares to its creditors.

Source: http://biz.yahoo.com/rb/070423/delta_results.html?v=5

12. *April 23, Department of Transportation* — **U.S. ranks second in world maritime container traffic.** The United States ranks second in world maritime container traffic with one in nine maritime containers in the world either bound for or coming from the United States, according to “America’s Container Ports: Delivering the Goods,” a new report from the Bureau of Transportation Statistics (BTS). BTS, a part of the U.S. Department of Transportation’s Research and Innovative Technology Administration, reported that U.S.–container trade in 2005 and 2006 was more than double the trade of a decade earlier. During that time, world container trade more than tripled, resulting in a decline in the U.S. share of world container trade from 16 percent to 11 percent. China has exceeded the U.S. share of world container trade since 1998.

Report: http://www.bts.gov/publications/americas_container_ports/.

Source: <http://www.dot.gov/affairs/bts1807.htm>

13. *April 23, Los Angeles Daily News* — **LAX risks losing its high profile.** Nothing may be more symbolic of the challenges facing Los Angeles International Airport (LAX) than the half-ton chunk of plaster that fell recently from its iconic theme restaurant, revealing layers of rust damage caused by years of neglect. Most of the existing structures were built in the 1960s and have been modernized only once, when the Bradley International Terminal was erected for the 1984 Olympics. But city officials have spent \$115million developing grandiose renovation plans that have gone nowhere. In recent months, however, LAX has gotten a bit more attention: A \$4billion upgrade was launched at the Bradley Terminal; a \$333million replacement of the south runway was completed; and the city approved spending \$1.8million to repair the landmark Encounter restaurant. And Los Angeles Mayor Antonio Villaraigosa is preparing to name a new executive director for Los Angeles World Airports — an administrator to oversee the department's \$1.2billion budget, resolve lingering disputes about airline and concession leases, and determine how LAX will accommodate a new generation of mega-jets. Options being considered include creating a special mid-field terminal with 40 extra gates for the jumbo jetliners. LAX serves nearly 17million travelers annually, second only to John F. Kennedy International Airport in New York City.

Source: http://www.dailynews.com/ci_5729365

14. *April 23, Canadian Press* — **Driver's license idea catching on in U.S., says Ontario tourism minister.** Ontario Tourism Minister Jim Bradley says the idea of using driver's licenses instead of passports at the Canada–U.S. border is gaining traction. Bradley — in a Washington meeting with officials at the State Department and the Department of Homeland Security — says the U.S. also recognizes the new security program can't be implemented all at once and there will have to be a transition period. Ontario is devising more secure driver's licenses. U.S. officials are plan to introduce the new rules by January 1, 2008, even though Congress gave them a 17-month reprieve.

Source: <http://www.canada.com/topics/news/national/story.html?id=f88>

15. *April 21, Houston Chronicle* — **Dallas-bound plane evacuated after bomb threat.** About 100 passengers were evacuated from a plane headed for Dallas on Saturday, April 21, after San Antonio International Airport received a bomb threat, authorities said. The airport received several calls this morning saying a bomb was in Terminal One, airport spokesperson David Hebert said. Around 10:30 a.m. CDT, a caller referred specifically to the Dallas-bound flight. The passengers were evacuated and the plane was taken to a safe zone where airport police and a canine unit found nothing following a search, Hebert said. The passengers were allowed to board again after a two-hour wait. The FBI is investigating, he said. The bomb threat was one of three made late Friday and early today in San Antonio during Fiesta, a 10-day citywide party.

Source: <http://www.chron.com/dispatch/story.mpl/front/4736973.html>

16. *April 20, Government Technology* — **Plans for cooperative airport employee screening.** The Transportation Security Administration (TSA), American Association of Airport Executives (AAAE), Airports Council International—North America (ACI-NA) and National Air Transportation Association (NATA) have announced plans to measurably maximize the effectiveness of screening employees at airports. The six-point plan to harden and bolster employee screening utilizes a risk-based approach. "Our strategy is to be nimble, flexible, mobile, and above all, dynamic," said TSA Administrator Kip Hawley. "Effective security requires partners working together within a network of overlapping measures around which terrorists cannot easily engineer. For that reason, we achieve a better overall security result by using our resources flexibly, not tied down at checkpoints checking and re-checking people that work at the airport every day." Over the next 90 days, TSA, ACI-NA, AAAE and NATA, through a working group, will develop the standards and solidify the implementation timeline for the plan. The plan will include testing of six key measures, followed by a phased rollout to the 452 commercial U.S. airports. The collaborative employee screening plan builds upon the layered approach already in place at the nation's airports, which includes perpetual vetting of employees against watch lists, badge and keypad-protected entry points, and TSA employee screening patrols and surges.

Source: http://www.govtech.net/magazine/channel_story.php/105106

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

17. *April 20, Associated Press* — **Agriculture officials impose moth quarantine in five California counties.** California agricultural authorities expanded their efforts to stop the spread of a voracious Australian moth Friday, April 20, by imposing a quarantine on the hundreds of plants the pest eats in a five-county region. The light brown apple moth, which feeds on

everything from grapes to eucalyptus trees, was spotted in the San Francisco Bay area on February 27, in what officials believe was its first appearance in the continental U.S. Since then, trappers have caught more than 170 of the invasive moths. The quarantine restricts the movement of more than 250 host plant species the moth eats in a 182–square mile region in portions of Alameda, Contra Costa, San Francisco, Marin and Santa Clara counties.

Source: <http://www.signonsandiego.com/news/state/20070420-2054-ca-mo-thinvasion.html>

[[Return to top](#)]

Food Sector

18. *April 23, Yonhap (South Korea)* — U.S. beef shipment arrives in South Korea. A shipment of U.S. beef arrived in South Korea on Monday, April 23, opening the door for the resumption of imports after a ban of more than three years due to concerns over mad cow disease. The 4.5 tons of meat from Kansas that arrived at Incheon International Airport will undergo quarantine inspections, the Ministry of Agriculture and Forestry said.

Source: <http://english.yonhapnews.co.kr/Engnews/20070423/91000000020070423110619E2.html>

19. *April 22, Associated Press* — E. coli outbreak sickens five in Pennsylvania. The state Health Department is investigating an E. coli outbreak that has sickened five people in four Pennsylvania counties. Health officials believe all the cases are linked to people who ate rare or medium–rare steak at different Hoss' Steak and Sea House restaurants in Centre, Dauphin, Venango and York Counties between March 24 and March 29. The restaurant exposures are the only common link among those who were sickened, the department said. Each ate a different cut of steak, but all requested it be cooked rare or medium–rare. Calvin B. Johnson, the state secretary of health, said his department was working with the state and federal agriculture departments to identify the source of the E. coli. The chain's affiliated meat processing facility, HFX Corp. of South Claysburg, PA, said it was recalling 259,230 pounds of beef as a precaution. Besides supplying meat for its Hoss' restaurants, HFX also processes beef for other restaurants and wholesalers. Nearly 5,000 pounds of the recalled beef was distributed to retail stores in Pennsylvania; the rest went to restaurants in Pennsylvania, Virginia, and West Virginia.

Source: http://www.philly.com/inquirer/local/pa/chester/20070422_E_coli_outbreak_sickens_5_in_central_Pennsylvania.html

20. *April 20, Associated Press* — Ground beef recalled after Napa children sickened by E. coli. California health officials on Friday, April 20, announced a recall in five states of frozen ground beef patties after at least three Napa County children who ate at Little League baseball snack shacks were sickened by E. coli. The recall was issued for about 100,000 pounds of frozen patties produced by Merced–based Richwood Meat Co. Inc. from April to May 2006 and distributed in California, Arizona, Idaho, Oregon and Washington. The products being recalled are hamburger patties and ground beef sold under the brands Fireriver, Chef's Pride, Ritz Food, Blackwood Farms, California Pacific Associates, C&C Distributing, Golbon and Richwood.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/04/20/state/n215610D17.DTL>

21. *April 19, U.S. Food and Drug Administration* — **Worldwide Fish & Seafood enters consent decree with FDA.** The U.S. Food and Drug Administration (FDA) Thursday, April 19, announced that Worldwide Fish & Seafood, Inc., Minneapolis, MN, (doing business as Coastal Seafood) a seafood processor and three of its officers have entered into a consent decree of permanent injunction due to violations of the Federal Food, Drug and Cosmetic Act. The consent decree requires the company to come into compliance with the act by developing and implementing adequate Hazard Analysis and Critical Control Point (HACCP) plans. The seafood HACCP regulations require that all seafood processors develop and implement adequate HACCP plans that identify all food safety hazards that are likely to occur for each kind of seafood product, and contain preventative measures that the processor can implement to control those hazards. Over six years, seven FDA inspections revealed that the defendants' HACCP plans were not adequate to prevent conditions that could pose a potential public health risk. In particular, the defendants' HACCP violations related to their failure to ensure that their seafood products were transported and continuously stored at adequate refrigeration temperatures to prevent bacteria growth and pathogen development. The decree allows FDA to order a shutdown, recall, or other corrective action in the event of future violations.
Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01613.html>

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

Water Sector

Nothing to report.

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

Public Health Sector

22. *April 23, BusinessWeek* — **AstraZeneca to buy MedImmune.** AstraZeneca PLC said Monday, April 23, it is buying U.S.-based biotech drugmaker MedImmune Inc. in a \$15.6 billion deal that will allow the British company to enter the vaccines market. The deal, which AstraZeneca hopes to close in June, will increase the company's proportion of biotechnology drugs in its pipeline from seven percent to 27 percent, and enlarge its total pipeline by 45 projects to 163 projects. That includes two late-stage products being developed by MedImmune, which is based in Gaithersburg, MD. The company has more than 2,500 employees in facilities across the U.S., Britain and the Netherlands. One product is a refrigerated formulation of its FluMist inhaled influenza vaccine. AstraZeneca's decision to enter the vaccines market follows the purchase of U.S. vaccines maker Chiron by Novartis AG last year.
Source: <http://www.businessweek.com/ap/financialnews/D8OM8LS00.htm>

23. *April 22, Agence France-Presse* — **New virus found in Australia deaths.** Australian doctors revealed Sunday, April 22, that three people who died shortly after receiving organ transplants from the same donor were all infected with a previously unknown virus. The virus was found in three Melbourne patients who died just weeks after they received organs from a 57-year-old man who suffered a fatal brain hemorrhage one week after returning from Europe. Australian officials said the infection was similar to lymphocytic choriomeningitis virus (LCMV), which

was linked to the deaths of several transplant patients in the U.S. last year. Mike Catton, from the Victorian Infectious Disease Laboratory, said tests carried out with the assistance of the Greene Infectious Disease Laboratory at Columbia University in New York looked at tissue samples taken from the dead transplant patients using new gene sequencing techniques. The new virus was found in all samples taken from the transplant recipients but not in tissue taken from the donor. Catton said doctors did not know yet how many people could be infected with the virus or whether it has killed anyone in the past.

Source: http://news.yahoo.com/s/afp/20070422/hl_afp/healthaustralia_070422120119;_ylt=Anz2yxFE0bML_sjh85f9.OyJOrgF

24. *April 20, U.S. Food and Drug Administration* — **FDA announces audio broadcasts on emerging drug safety information.** The U.S. Food and Drug Administration (FDA) is alerting health care professionals and consumers to the availability of audio broadcasts that provide emerging drug safety information. The broadcasts can be transmitted to personal computers and personal audio players. The service is part of the agency's ongoing effort to broaden and speed its communications concerning the safety of marketed medications when unexpected adverse events are reported to FDA. The broadcasts are an addition to FDA's traditional print- and Web-based public health advisories (PHAs).

Subscription information: <http://www.fda.gov/cder/drug/podcast/default.htm>

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01614.html>

25. *April 20, Canadian Press* — **Outbreak of the mumps continues in Nova Scotia.** Public health officials in Nova Scotia, Canada, are reporting another jump in an outbreak of the mumps as they investigate 120 cases across the province. The majority of cases remain in the 20–25 age group. The Public Health Agency of Canada says in an average year there are 30 to 80 cases of the mumps across the entire country.

Source: <http://www.hfxnews.ca/index.cfm?sid=24122&sc=89>

26. *April 20, Journal of Biological Chemistry* — **Identification of an in vivo inhibitor of Bacillus anthracis spore germination.** Germination of Bacillus anthracis spores into the vegetative form is an essential step in anthrax pathogenicity. This process can be triggered in vitro by the common germinants inosine and alanine. Kinetic analysis of B. anthracis spore germination revealed synergy and a sequential mechanism between inosine and alanine binding to their cognate receptors. Because inosine is a critical germinant in vitro, we screened inosine analogs for the ability to block in vitro germination of B. anthracis spores. Seven analogs efficiently blocked this process in vitro. This led to the identification of 6-thioguanosine, which also efficiently blocked spore germination in macrophages and prevented killing of these cells mediated by B. anthracis spores. 6-Thioguanosine shows potential as an anti-anthrax therapeutic agent.

Source: <http://www.jbc.org/cgi/content/abstract/282/16/12112?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&fulltext=anthrax&andorexactfulltext=and&searchid=1&FIRSTINDEX=0&sortspec=date&resource type=HWCIT>

[[Return to top](#)]

Government Sector

27. *April 23, Government Computer News* — **USA.gov gets redesign to boost usability.** The General Services Administration (GSA) last week unveiled a redesign of USA.gov, the federal government's official Web portal. The site, which was launched early this year as a replacement for FirstGov.gov, provides a centralized place to find government information online. USA.gov lets visitors search for information on hundreds of government services, from checking tax refund status to contacting elected officials. The agency based the changes on the results of usability testing and other user feedback. GSA wants to make the site clearer and easier to use by reducing page clutter; adding images to news and feature stories; specifically tailoring the Spanish-language version of the site, GobiernoUSA.gov, to the Latino community; and making it easier to change the font size. The redesign also added visual cues to make it clear that USA.gov is the official U.S. government Web portal. For example, it posts a crisp image of the U.S. flag, as well as the Great Seal of the United States and the White House, on every page.

Source: http://www.gcn.com/online/vol1_no1/43545-1.html

28. *April 23, Tartan Online (PA)* — **Suspicious package causes lock down on campus.** A suspicious package was identified Thursday afternoon, April 19, on the Carnegie Mellon campus behind Hamburg Hall. The package, a three-foot-tall silver and green metal cylinder, was spotted by a student who immediately called 911. At about 12:30 p.m. EDT, a car belonging to the Pittsburgh Bureau of Police chased a suspicious vehicle into the Forbes Avenue driveway and pulled it over in front of Newell-Simon Hall. Shortly thereafter, several unmarked police cars barricaded the suspicious vehicle in front of the Collaborative Innovation Center. The university did not issue an official evacuation notification, but police briefly locked down the campus while they conducted an investigation. The Allegheny County Bomb Squad, the Pittsburgh Bureau of Police, Carnegie Mellon University Police, and University of Pittsburgh Police were all present on the scene. The bomb squad investigated the package and confirmed that it was a facsimile of a weapon of mass destruction. Though the squad declared the package harmless, the squad also checked the interior of Hamburg Hall and used bomb-sniffing dogs to ensure that there were no hidden bombs in the area.

Source: http://thetartan.org/2007/4/23/news/bomb_threat

[[Return to top](#)]

Emergency Services Sector

29. *April 23, Associated Press* — **Louisiana National Guard communications system ready for next storm .** With the next hurricane season quickly approaching, the Louisiana National Guard says the state's new high-tech communication system is ready to go in case of disaster. In the days after Hurricane Katrina, nearly every state and federal agency could not communicate during the desperate days of search and rescue operations. The new system allows soldiers to talk to each other, as well as bring in other emergency agencies to communicate on the same system. If traditional communication systems are wiped out, the Guard would now be able to access the Internet and tap into such Websites as Army Knowledge Online, which is a secure military site that would allow Louisiana soldiers to write and transmit images to show the extent of the disaster immediately to supporting military units outside of the state. On Saturday, April 21, the National Guard tested the communications systems in a statewide exercise in which it simulated a Category 2 hurricane striking Vermilion,

Iberia and Lafayette parishes. Beyond expected minor glitches, the system worked well, said Colonel Ronnie Johnson, the National Guard's commander of the 256th Brigade Combat Team. Source: <http://www.katc.com/Global/story.asp?S=6409205>

30. *April 23, United States Joint Forces Command* — **Noble Resolve 07 begins in Virginia.** U.S. Joint Forces Command (USJFCOM) kicked off its series of experiments in Virginia Monday, April 23, aimed at enhancing homeland defense measures and military support in the event of a natural or man-made disaster. Noble Resolve, sponsored by USJFCOM, is an experimentation campaign plan supported by U.S. Northern Command (NORTHCOM) to develop solutions for U.S. agencies and organizations by providing the means to deter, prevent, and defeat threats and aggression aimed at the U.S., its territories, and interests. This week's event, known as Noble Resolve 07-1, is the first of what will be a series of experiments to be held over a number of years on this topic. Noble Resolve 07-1 is a week-long event that will bring more than 125 people from across the United States and a number of other countries to develop solutions to provide improved defense support to civil authorities and build upon global partnerships. Throughout the Noble Resolve campaign, USJFCOM will also partner with the U.S. Transportation Command, and other federal agencies such as the Dept. of Homeland Security, the FBI and Customs and Border Protection. It will also team with individual states, as well as multinational participants. Source: <http://www.jfcom.mil/newslink/storyarchive/2007/pa042307.htm>

31. *April 22, Stamford Advocate (CT)* — **First responders in Connecticut drill for disaster.** The hundreds of emergency workers gathered in South Norwalk, CT, for one of the state's largest disaster drills got word just after 9:00 a.m. EST Saturday, April 21, that a large explosion had derailed a Metro-North train. Inside the train cars, about 100 volunteers feigning injuries or death awaited evacuation. The drill, Metro-North Ready Region 2007, involved about 400 emergency service workers and scores of truck drivers coordinating their response to the mock explosion. Norwalk police and firefighters helped with evacuations, while Stamford Bomb Squad personnel donned 80-pound suits to defuse a second mock bomb found on the train, intended to kill emergency workers responding to the blast that rocked the train off its tracks. This drill also involved all departments at Norwalk Hospital. As injured riders were carried off the train, hospital administrators implemented their emergency-preparedness plan, counting available beds, stationing security officers at hospital entrances, and establishing command centers in the hospital. Observations by dozens of evaluators will be examined over the next few weeks and a final report on the drill -- which will include recommendations for improvements -- will be issued. Source: <http://www.stamfordadvocate.com/news/local/scn-sa-nor.disaster6apr22.0.5833000.story?coll=stam-news-local-headlines>

32. *April 22, Tennessean* — **Tennessee's Office of Homeland Security to coordinate seven county exercise.** The Tennessee Office of Homeland Security will conduct an emergency preparedness exercise on Tuesday, April 24. Jeremy Heidt, spokesperson with the Tennessee Emergency Management Agency, said that the exercise will simulate conditions where treatment and medications would have to be distributed to a large number of people, such as a pandemic. Forty-seven agencies and more than 300 volunteers will support the exercise. Simulated medications will be distributed to the volunteers in response to the exercise scenario. Source: <http://www.tennessean.com/apps/pbcs.dll/article?AID=/2007042>

[[Return to top](#)]

Information Technology and Telecommunications Sector

- 33. *April 23, USA TODAY* — Cyberspies exploit Microsoft Office.** Cyberspies have a new secret weapon: tainted Microsoft Office files. A rising number of cyberattacks are taking aim at specific individuals at critical government agencies and corporations — enticing them to unwittingly open a corrupted Word, Excel or PowerPoint file sent as an e-mail attachment. Clicking on the file relinquishes control of the PC without the user's knowledge. The attacker then uses the compromised PC as a base from which to roam the organization's internal network. Federal agencies and defense and nuclear contractors are under assault. Security firm MessageLabs says it has been intercepting a series of attacks from PCs in Taiwan and China since November. In early 2006, security experts detected one or two such attacks a week. Last month, MessageLabs intercepted 716 e-mails carrying corrupted Office files aimed at 216 different agencies and companies. Assaults are coming from China and perhaps other countries in the hunt for military, trade and infrastructure intelligence, says Alan Paller, research director at The SANS Institute, a security think tank. The goal: strategic advantage over the USA. "The attacks are working," says Paller. "Penetrations are deep and broad."
Source: http://www.usatoday.com/tech/news/computersecurity/2007-04-22-cyberspies-microsoft-office_N.htm
- 34. *April 23, eWeek* — Oracle issues database patch postponed for testing.** Oracle has released a missing fix for the database flaw rated most deadly in the Critical Patch Update the company released last week. The flaw, dubbed DB01 in the update issued April 17, is in the Core RDBMS (relational database management system) and can be remotely exploited over the network by an attacker sans user identification or password authentication. The flaw is specific to the Windows operating system and affected the 9.2.0.8 version of the database. On Friday, April 20, Eric Maurice of Oracle posted a note on a company blog announcing the Critical Patch Update for the Windows 32-bit version of the 9.2.0.8 database is now available.
Oracle blog: <http://blogs.oracle.com/security/2007/04/20#a59>
Source: <http://www.eweek.com/article2/0.1895.2120914.00.asp>
- 35. *April 20, IDG News Service* — Hacker shows Mac break-in.** A hacker managed to break into a Mac and win a \$10,000 prize as part of a contest started at the CanSecWest security conference in Vancouver. In winning the contest, he exposed a hole in Safari, Apple's browser. "Currently, every copy of OS X out there now is vulnerable to this," said Sean Comeau, one of the organizers of CanSecWest. The conference organizers decided to offer the contest in part to draw attention to possible security shortcomings in Macs. Initially, contestants were invited to try to access one of two Macs through a wireless access point while the Macs had no programs running. No attackers managed to do so, and so conference organizers allowed participants to try to get in through the browser by sending URLs via e-mail. Dino Di Zovie, who lives in New York, sent along a URL that exposed the hole. Because the contest was only open to attendees in Vancouver, he sent it to a friend who was at the conference and forwarded it on. The URL opened a blank page but exposed a vulnerability in input handling in Safari.
Source: http://www.infoworld.com/article/07/04/20/HNmachackedatconference_1.html

36. April 20, IDG News Service — Kickbacks on federal IT contracts widespread, involved millions, DOJ charges. An alleged multimillion-dollar kickback scheme involving work on numerous U.S. government contracts touches dozens of IT vendors and systems integrators, according to court documents unsealed Friday, April 20. The allegations set up a major confrontation between the U.S. government and virtually the entire U.S. IT industry. The U.S. Department of Justice (DOJ) filings list improper kickbacks on a number of contracts, including ones from the U.S. Army, the Air Force, the FBI, the Department of State, the General Services Administration, the Department of Education and the U.S. Postal Service. The DOJ announced it had joined three whistle-blower lawsuits against Hewlett-Packard Co., Sun Microsystems Inc. and Accenture Ltd. The DOJ's complaints allege that the three companies, through "alliance partnerships" with dozens of other vendors, exchanged millions of dollars in illegal rebates and other payments since the late 1990s. The DOJ complaints accuse Accenture and other systems integrators of collecting money from IT vendors in exchange for preferential treatment on government contracts they were working on, or exchange for strong recommendations to potential government customers. The defendants did not report these kickbacks to the U.S. government, the DOJ alleges.
DOJ press release: http://www.usdoj.gov/opa/pr/2007/April/07_civ_265.html
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017361&intsrc=hm_list

37. April 20, Network World — Nortel warns of three VPN Router product flaws. Nortel last week warned of several backdoors, and other flaws, in its VPN and secure routing products that could allow unauthorized remote access to an enterprise network. User accounts used for diagnostics on Nortel VPN routers (formerly known as Contivity) could be used to gain access to a corporate VPN. In another potential vulnerability, unauthorized remote users could also gain administrative access to a VPN router through a Web interface. A third vulnerability could result in someone cracking users' VPN passwords. Nortel says it has issued software that fixes these flaws. Product versions affected include all Nortel VPN router models — 1000, 2000, 3000, 4000 and 5000.
Source: <http://www.networkworld.com/news/2007/042007-nortel-vpn-router-flaw.html>

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

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.