



Department of Homeland Security Daily Open Source Infrastructure Report for 24 May 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

- The Associated Press reports the Wildlife Center of Virginia is developing a national surveillance network that would help detect diseases in wildlife that may be linked to bioterrorism. (See item [24](#))
- The American Red Cross has released a report that summarizes the results of a New York City survey indicating that while most New York residents have taken important preparedness actions, there is still more work to be done. (See item [31](#))

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. **May 23, Reuters** — **Oil surges above \$70 on commodity rebound.** Oil surged above \$70 on Tuesday, May 23, as commodities staged a modest recovery from last week's sell-off, Venezuela mooted OPEC oil production cuts, and the U.S. government predicted another rough Atlantic hurricane season. U.S. crude for July delivery rose 82 cents to \$70.78 a barrel. The U.S. National Oceanic and Atmospheric Administration said 2006 could see up to 10 hurricanes. About 20 percent of the Gulf's 1.5 million barrels per day (bpd) of crude oil output, along with 13 percent of the region's 10 bcfd of natural gas production, has been shut since the record 2005 storm season that pushed U.S. crude above \$70 for the first time. Venezuelan Oil

Minister Rafael Ramirez said healthy global crude stockpiles would justify a reduction in full-throttle output limits when the Organization of the Petroleum Exporting Countries meets next week. Rising U.S. gasoline inventories could provide some relief from high prices, with a Reuters poll predicting a fourth consecutive weekly jump — by an average 1.4 million barrels — when government data is released on Wednesday. Refineries are cranking up production before the Memorial Day holiday weekend, the traditional launch of the U.S. summer gasoline season.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/23/AR2006052300202.html>

2. **May 22, Associated Press — Iowa company hopes to make gasoline obsolete.** While much of the world fumes over escalating fuel prices, a small company in Iowa is quietly hoping to make gasoline obsolete as an engine fuel. Research at the Hydrogen Engine Center Inc., led by a retired Ford Motor Co. engineer, hopes to meet Environmental Protection Agency automotive 2007 emission standards with an engine that can run on a number of fuels including hydrogen, ethanol, natural gas, propane, or digester gas from landfills. The company is making more efficient, environmentally friendlier engines to replace those used in generators and in forklift trucks, airline ground equipment, irrigation pumps, tractors and buses. Ford, General Motors, and Chrysler have dropped industrial engine production as they've cut costs, leaving what Hollinger said is a ready-made market for his fledgling company. Brad Van Horn, an engine distributor with Northern Power Productions, said some orders are already placed for the generators as they approach the production phase. "The level of excitement is huge," he said. Airports needing to replace the Ford engines in their baggage handling and other equipment will also be a large market. The company said American Airlines alone has 9,500 vehicles likely to be converted to alternative fuels over the next decade.

Source: <http://www.enn.com/today.html?id=10504>

3. **May 22, Reuters — FTC gasoline price probe finds nothing illegal.** The U.S. Federal Trade Commission (FTC) said on Monday, May 22, it had found no evidence that oil companies illegally manipulated gasoline prices or constrained oil refining capacity to restrict supply. The investigation found some instances of questionable gasoline price increases in the wake of Hurricane Katrina last year, but no evidence that companies helped foster a run-up in prices since 2002 by restricting refining capacity or cutting inventory, the FTC said. The probe concluded that the spike in gasoline prices after Katrina hit in late August and Hurricane Rita in September, was in line with "standard supply-and-demand model of a market performing competitively." The FTC defined price gouging as any rise in price that occurs without a corresponding increase in cost or other explanation. Many states have laws against price gouging, but there is no federal law against excessive price increases. The FTC expressed skepticism about passing such a law, saying it would be difficult to define and enforce.

Source: http://news.yahoo.com/s/nm/20060522/us_nm/energy_gasoline_ftc_dc_3

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

Chemical Industry and Hazardous Materials Sector

4. **May 24, WTSP (FL) — Diesel fuel spill prompts road closure in Florida.** Hillsborough County, FL, Fire Rescue units and private contractors cleaned up 800 gallons of diesel fuel that

spilled from a tanker when it overturned on the Causeway Boulevard Tuesday morning, May 23. The road was kept closed until mid-afternoon.

Source: <http://www.wtsp.com/news/local/morning/article.aspx?storyid=31775>

5. *May 23, Hopewell News (VA)* — **Plant releases chemical particulate during electrical failure.** Hopewell, VA's, Smurfit-Stone plant are trying to calm the fears of some residents whose vehicles were dusted Sunday, May 21, with particulate residue consisting of sodium sulfate/sodium carbonate from a chemical air release. An electrical failure in a precipitator allowed the release, which, when detected, was stopped through a process shutdown.

Source: http://208.62.60.4/30/article_724.shtml

6. *May 23, Pioneer Press (MN)* — **Chemical leak from rail tanker prompts evacuation, road closure in Minnesota.** Hydrochloric acid leaked from a rail tanker car Tuesday, May 23, in an industrial area east of downtown St. Paul, MN, prompting authorities to evacuate the area and close a stretch of Warner Road. Three people were treated at the scene for chemical exposure. Officials said they did not know what caused the leak, which happened at Hawkins Inc.

Source: http://www.twincities.com/mld/pioneerpress/news/local/146484_22.htm

7. *May 22, Associated Press* — **Oklahoma officials investigate cause of acid leak.** Dozens of people in Wynnewood, OK, were allowed to return to their homes Sunday morning, May 21, at their own risk after an acid vapor leak at a local refinery sent potentially dangerous fumes floating through the air. Residents of about 45 homes, located five blocks north of the Gary-Williams Co. refinery, were evacuated Saturday evening, May 20, Garvin County Undersheriff Steven Brooks said. About a week ago, the same plant caught on fire and about 150 people were temporarily evacuated from their homes. Saturday's leak of hydrogen fluoride may be related to last week's fire, Brooks said.

Source: <http://www.kotv.com/main/home/stories.asp?whichpage=1&id=104649>

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

Defense Industrial Base Sector

8. *June 01, National Defense* — **Marine Corps procurement forecast clouded by bleak budget projections.** The prospect of tighter defense budgets is arriving at a time when the Marine Corps is struggling to repair and replace equipment lost or damaged in recent fighting, and to restore its combat readiness. "If we get involved in another major operation any time soon, we could have a severe problem," said Brig. Gen. Raymond C. Fox, assistant deputy commandant for programs and resources. The rebuilding process will cost about \$12 billion and take at least two years. The Corps has asked for \$6 billion to get started in 2007. To get a clearer idea of what kinds of equipment and personnel the Corps will need a decade from now, Commandant Gen. Michael Hagee has commissioned a "capabilities assessment" that is scheduled to be completed this summer. Equipment buys in the near term will focus on technologies to defeat improvised explosive devices and on protective systems for troops and vehicles.

Source: <http://www.nationaldefensemagazine.org/issues/2006/June/MarineCorps.htm>

9.

May 22, European Defense Agency — **New European defense equipment market to be launched in July.** The new European defense equipment market will be launched on Saturday, July 1, with the participation of all but three of the 25 European Union (EU) Member States. "This regime will create new opportunities for companies across Europe, strengthen our defense technological and industrial base and offer better value for money to the armed forces and to taxpayers," said European Defense Agency Chief Executive Nick Witney. The market will operate on the basis of the Code of Conduct on Defense Procurement, a voluntary, inter-governmental regime, approved by Defense Ministers last November to cover defense equipment purchases which are exempt from the normal cross-border competition rules of the EU single market.

Source: <http://eda.eu.int/news/2006-05-22-0.htm>

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

Banking and Finance Sector

10. *May 23, Kyodo News (Japan)* — U.S. Treasury: North Korea still counterfeiting U.S. dollars. North Korea is continuing to counterfeit U.S. dollars, a U.S. Treasury official said Monday, May 22. "We do believe that they are continuing to counterfeit U.S. currency," Daniel Glaser, U.S. deputy Treasury assistant secretary for terrorist financing and financial crime, told a forum sponsored by the Institute for Korean-American Studies. Glaser did not indicate whether the alleged counterfeiting activities were being carried out in connection with Banco Delta Asia SARL, a Macao-based bank currently being investigated by U.S. authorities over its ties to North Korean counterfeiting and money-laundering operations. The Treasury Department last September designated Banco Delta Asia as a primary money-laundering concern, barring U.S. financial institutions from dealing with it and leading the Macao government to freeze bank accounts tied to North Korea.

Source: <http://asia.news.yahoo.com/060522/kyodo/d8hp3s180.html>

11. *May 23, Jakarta Post (Indonesia)* — Shop owner arrested for cybercrime. The owner of a small computer shop in Jakarta, Indonesia, was able to get through the electronic defense system of one of the city's major banks, police said Monday, May 22. The man entered fictitious credit card transactions into the city's second largest bank system, Bank Central Asia (BCA). The suspect used no sophisticated technology. He just used seven cards to authorize 12 transactions totaling U.S. \$47,222. Most of the Visa and Mastercard cards were issued by foreign banks, including Prudential, Westpac, and ANZ. Police suspect TL got the credit card numbers from recording the details of customers' past transactions, though he could have broken into the bank's computer system. The vice chairman of the Indonesian Telecommunications Community, Mas Wigrantara, said that at least 1,000 incidents of e-banking fraud, virus uploads, and hacking activities had been reported in the last six months. "Although the number is significant, banks are reluctant to report cases to police because they are worried it will affect their reputation and the public will no longer trust e-banking," he said. Wigrantara said the Indonesia Computer Security Incident Response Team was not having much of an impact because of the limited number of cases reported.

Source: <http://www.thejakartapost.com/detailcity.asp?fileid=20060523.C02&irec=2>

12.

May 22, NBC4i.com (OH) — **Seven executives indicted in \$3 billion fraud scheme.** A group of former executives with Dublin, OH–based National Century Financial Enterprises was indicted Monday, May 22, on charges that they committed a \$3 billion fraud from the company's investors. The group of former executives was named in the 60–count indictment, which includes charges of conspiracy, securities fraud, wire fraud, mail fraud, and money laundering, NBC 4's John Ivanic reported. The indictment seeks about \$2 billion in forfeiture of property involved in the money laundering conspiracy, officials said. The seven people are accused of conspiring to defraud investors by lying to them and others about how the investors' fund would be used, diverting the funds, and then hiding the shortfall by moving the money back and forth between subsidiaries' bank accounts and creating phony reports and records to cover up the scheme. In November 2002, agents with the Federal Bureau of Investigation raided the Dublin offices, and seized financial statements, computer programs and e–mails that helped build a massive fraud case against 10 employees. Investigators said National Century would make loans to businesses by buying their accounts receivables, most notably, health care providers. Officials said the case is the largest of its kind in U.S. history.

Source: <http://www.nbc4i.com/news/9254246/detail.html>

13. *May 22, SC Magazine* — **Iowa phisher gets 21 months in jail.** An Iowa man, guilty of using phishing schemes to dupe as many as 250 MSN customers into giving up their personal information, was sentenced Friday, May 19, to 21 months in prison. Jayson Harris ran a phishing scheme by sending e–mails to MSN users asking them to visit a bogus Website to update personal information. The e–mails promised the recipients a 50 percent discount on their next bill, according to published reports. Fifty to 250 people fell for the attack, which netted Harris about \$57,000. Occurring between January 2003 and June 2004, the phishing scheme was the first of its kind investigated by Microsoft's Internet Safety Enforcement Team. Since then, the team has investigated more than 120 phishing reports.

Source: <http://www.scmagazine.com/uk/news/article/560357/iowa+phisher+gets+21+months+jail/>

[[Return to top](#)]

Transportation and Border Security Sector

14. *May 23, Associated Press* — **Plastic surgeon helps restrain unruly air passenger.** An elderly man on an American Airlines flight was restrained by passengers, including television's Dr. Robert Rey ("Dr. 90210"), after he got out of his seat and shoved a flight attendant late Monday, May 22, officials said. The jetliner landed safely in Los Angeles and police took the 80–year–old man, who did not speak English, to a hospital for a 72–hour mental observation, said airport spokesperson Nancy Castles. "He evidently started to panic about 15 minutes before landing, when everyone is supposed to be buckled into seats," Castles said. None of the five crewmembers or 122 passengers aboard the MD–80 plane from Austin, TX, reported injuries, American Airlines spokesperson Billy Sanes said. Rey, a plastic surgeon who practices martial arts, said he got out of his seat and intervened when he heard the man make a "big noise" as he pushed a female flight attendant toward the cockpit.

Source: <http://www.cnn.com/2006/US/05/23/airline.disturbance.ap/index.html>

15.

May 23, Department of Transportation — **The U.S. private sector should get involved in transportation investments to help fight congestion.** U.S. investors, including financial, construction and engineering firms, must begin investing in highway, airport, and transit projects to help keep pace with the demands of a rapidly growing economy, Department of Transportation Secretary Norman Y. Mineta said on Tuesday, May 23, at the NASDAQ market in New York City. Mineta was in New York to outline a new national congestion relief initiative,” National Strategy to Reduce Congestion on America’s Transportation Network,” and discuss the role the private sector will play in the new plan. He warned that congestion was costing America \$200 billion a year, that traffic jams alone waste 2.3 billion gallons of gasoline and 3.7 billion hours each year and that airline delays were robbing the economy of \$9.7 billion annually. He announced that the Department of Transportation was launching an effort to educate state and local officials about the new concept of private transportation financing, adding that he will work to encourage more states to pass the legislation needed to attract billions in new funding, investment, and management of transportation projects. To download a copy of the plan: <http://isddc.dot.gov/OLPFiles/OST/012988.pdf> Mineta's speech: <http://www.dot.gov/affairs/minetasp052306.htm>. Source: <http://www.dot.gov/affairs/dot6406.htm>

16. *May 23, Associated Press* — **Pride of Hawaii to make its way to the islands from California.** The Pride of Hawaii, the largest and most expensive U.S.–flagged passenger ship ever built, left California on Tuesday, May 23, for its new home in the islands. The 2,400–passenger cruise ship was christened Saturday, May 20, in Los Angeles, and is expected to arrive at its Honolulu homeport on June 3. The Pride of Hawaii will officially enter seven–day interisland service June 5. The 965–foot vessel is the third in a series of U.S.–flagged cruise ships sailing under the NCL America brand for the rapidly growing interisland market. The ship weighs 93,500 tons and cost more than \$500 million to build. It will employ a crew of more than 1,000, boosting NCL's U.S.–flagged fleet to about 4,000. NCL's fleet in Hawaii is projected to bring Hawaii's cruise passenger carryings to more than 650,000 a year by 2007. At those levels, Hawaii will be comparable in size to Alaska as a cruise destination. Source: http://www.usatoday.com/travel/news/2006-05-23-pride-of-hawaii_x.htm

17. *May 23, National Defense Magazine* — **Complications of airline technology.** As the Department of Homeland Security (DHS) continues to pay for tests on systems designed to thwart shoulder–fired missiles from taking down commercial airliners, a potential barrier looms: Any time a U.S. commercial aircraft carrying such technology flies overseas, it would be in violation of federal laws prohibiting the export of military technology. DHS is currently in phase three of a congressionally mandated program to test the feasibility of laser–based counter missile systems. Affordability, maintenance costs, and logistical concerns are seen as some of the major roadblocks to implementation. The Arms Export Control Act and its International Traffic in Arms Regulations, better known as ITAR, regulates the export of military technology overseas. “If you put this technology on a commercial airplane, as soon as you fly overseas, you’ve exported it,” said James Tuttle, DHS program executive for the aircraft protection program, said at an Institute for Defense and Government Advancement conference. “We know some laws are going to have to change, but we want to make sure we are protecting the technology,” Tuttle said. Tamper–proof seals on the devices would be a possible solution, he added. When testing is complete, Congress will have to decide whether to fund the system.

Source: <http://www.nationaldefensemagazine.org/issues/2006/June/SecurityBeatJune.htm>

18. *May 23, Associated Press* — Flights from Venezuela resume after stoppage by volcano.

Airline officials in Venezuela said on Monday, May 22, that flights to the United States had resumed after a cloud of volcanic ash in the Caribbean suspended some international flights over the weekend. American Airlines' flights were beginning to operate normally again Monday, the Fort Worth-based company's director in Venezuela, Omar Nottaro, told Union Radio. Venezuela's largest carrier, Aeropostal, said it restored full operations between Caracas and Miami on Monday. A dome atop a volcano on Montserrat island collapsed Saturday, May 20, sending volcanic debris cascading down the mountain and shooting ashes 10 miles into the sky. A huge cloud of ash billowing from the volcano forced the suspension of flights to Miami, Aruba, Cuba, Curacao, and other destinations Sunday.

Source: http://www.usatoday.com/travel/flights/2006-05-23-volcano-flights_x.htm

19. *May 19, Puget Sound Business Journal (WA)* — Alaska Airlines saves fuel money. At this week's Alaska Air Group's shareholders' meeting at the Museum of Flight in Seattle, CEO Bill Ayer said the company's fuel-hedging strategy is working. Although a barrel of oil costs around \$68 right now, Alaska is paying \$41 a barrel for about half of its fuel this year thanks to its hedging strategy. The airline's fuel hedges will expire at the end of 2008.

Source: <http://seattle.bizjournals.com/seattle/stories/2006/05/15/daily38.html>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

20. *May 23, Agricultural Research Service* — Quicker test for turkey viruses. A new, highly sensitive diagnostic test to detect viruses associated with poult enteritis complex (PEC) has been developed by Agricultural Research Service (ARS) scientists. This disease of young turkeys causes diarrhea, poor weight gain and, in some cases, high mortality. Microbiologists developed the test in a format that allows the detection of several types of viruses at one time. The test relies on a molecular technique called real-time reverse transcription-polymerase chain reaction (RRT-PCR), which is a highly sensitive and specific method for detecting viral RNA. Current diagnostic methods for PEC-associated viruses have limitations because of poor analytic specificity and sensitivity. The researchers inoculated turkey poults with each of the PEC-associated viruses and later collected intestinal tissue samples and cloacal swabs from the experimentally infected birds. The RRT-PCR test showed high sensitivity, accurately detecting the target viruses in both the tissues and swabs. While intestinal samples have previously been essential to making a definitive PEC diagnosis, the researchers found that cloacal samples—which are easier to collect and process—were just as suitable for testing. Using them will not only save time and money, it will also eliminate the need to euthanize birds for sampling.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

21. *May 23, Telegraph (United Kingdom)* — **Fungus threatens banana.** The most popular type of banana, the Cavendish, is under threat from disease. In the 1950s, people ate a different banana, the Gros Michel but it was wiped out by Panama disease. Now the Cavendish could follow suit as a new strain of the fungus to which it was supposed to be immune has begun to attack the plants. So far, the new, more aggressive variant of Panama disease — TR4 — has not reached the main exporting countries in Latin America or Africa but it is spreading widely through Cavendish plantations in Asia — Indonesia, Taiwan, southern provinces of China and Malaysia. In the humid conditions of traditional banana plantations in Central America, the black Sigatoka fungus which attacks leaves, also thrives and the plants must be protected by weekly sprays of fungicides.

Source: <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/05/23/wnana23.xml&sSheet=/news/2006/05/23/ixnews.html>

[[Return to top](#)]

Food Sector

22. *May 22, U.S. Food and Drug Administration* — **Salads recalled.** Mrs. Gerry's Kitchen, Inc. of Albert Lea, MN, is voluntarily recalling approximately 54,000 pounds of salads because it has the potential to be contaminated with harmful bacteria. No illnesses have been reported to date. These products have been sold under the following brands: Mrs. Gerry's, SYSCO, Knowlan's (Festival), Spoon River, and Fareway. Affected product was distributed to a few distributors in the states of UT, ND, SD, NE, MN, IA, WI, IL, MI and reached consumers through a variety of distribution avenues including retail stores, foodservice and wholesale distributors.

Source: http://www.fda.gov/oc/po/firmrecalls/gerrykitchen05_06.html

23. *May 19, U.S. Food and Drug Administration* — **Salads, spreads, and dips recalled.** House of Thaller, Inc. of Knoxville, TN, is recalling approximately 160,000 pounds of Ham Salad, Chicken Salad, Turkey Salad, Tuna Salad, Seafood Salad, Seafood Salad Mix, Pea Salad Mix, Shrimp Salad, Artichoke Shrimp Dip, Crab Dip, Cajun Crab Dip because it has the potential to be contaminated with harmful bacteria. These products are being recalled because a supplier provided an ingredient that was not processed in a manner to prevent the growth of harmful bacteria. These products have been sold under the following brands: Brand names included are House of Thaller, Kroger Brand, Mrs. Gerry's, Dairy Fresh, The Fresh Market, Southern Gourmet, and Southern Style. Affected product was distributed to FL, IN, MI, MN, NC, OH, TN, TX and reached consumers through a variety of distribution avenues including retail stores, and wholesale distribution centers.

Source: http://www.fda.gov/oc/po/firmrecalls/thaller05_06.html

[[Return to top](#)]

Water Sector

Nothing to report.

Public Health Sector

24. May 23, Associated Press — Network would help detect bioterrorism. The Wildlife Center of Virginia is developing a national surveillance network that would help detect diseases in wildlife that may be linked to bioterrorism. While there are already systems designed to detect diseases in humans and domestic animals, Project Tripwire would be the first comprehensive effort to monitor wildlife for signs of bioterrorism, Wildlife Center President Ed Clark said Monday, May 22. The Wildlife Center entered into a \$166,000, six-month contract with the Institute for Defense and Homeland Security last month to plan a database that would initially link 20 to 25 of North America's largest wildlife hospitals. The hospitals would enter information about animals they treat into the database, which would be programmed to pick up statistical anomalies, such as a higher-than-usual number of animals in one area suffering from an infection. Anything that could be the result of bioterrorism would be reported to the Department of Defense, the Centers for Disease Control and Prevention, and other federal and state agencies.

Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1137836259739&path=!news&s=1045855934842

25. May 23, Associated Press — Treatments for neglected diseases urged. The sickness starts with the bite of a tiny sand fly and mutates quickly from there — chills, then fever, then an onslaught of black lesions that will most likely prove fatal within six months without treatment. Known as kala azar — a Hindi word meaning Black Death — the disease has killed more people than the 21-year civil war in Sudan, many of them extremely poor children. With the United Nations' 192-member World Health Assembly meeting in Switzerland, the governments of Kenya and Brazil have sent a resolution asking the panel to urge governments to set drug research priorities based on disease burden. According to the UN, less than 10 percent of investment in health research goes to diseases that affect 90 percent of the world. The disease causes high fever, swelling of the spleen and massive weight loss. Around 500,000 new cases appear every year in the world, with a sharp increase in the last decade, according to the World Health Organization. There have been precious few advances in kala azar drugs in nearly two decades. The problem, critics say, is that there's little financial incentive to develop drugs for people who will never be able to pay for them.

Source: <http://www.latimes.com/news/nationworld/world/wire/sns-ap-af-rica-neglected-diseases.1.3445036.story?coll=sns-ap-world-headlines>

26. May 23, Agence France-Presse — Virus mutation linked to spread of chikungunya disease. French researchers said an epidemic of the disease known as chikungunya, which ravaged the Indian Ocean island of Reunion, was spurred by a mutated form of a mosquito-borne virus. The chikungunya virus is typically spread by the yellow fever mosquito (*Aedes aegypti*). But sequencing of a gene, E1, which allows the virus to attach to mosquito cellular membranes, suggests the pathogen may also be carried by another species, the Asian tiger mosquito (*Aedes albopictus*). The Pasteur Institute team analyzed samples of the virus taken from 121 patients in Reunion, Madagascar, Seychelles, Mayotte, and Mauritius. The outbreak of chikungunya began in Reunion in early 2005 but dramatically accelerated in

December. Eventually, around 258,000 people — a third of the island's population — fell sick with the disease, which also claimed 219 lives directly or indirectly. The French scientists say the mutated form appears to have emerged in September 2005 and within a few months swiftly became the dominant viral strain in the epidemic. Around 6,000 other cases of illness have been recorded in Madagascar, Seychelles, Mauritius, and Mayotte.

Genome Microevolution of Chikungunya Viruses Causing the Indian Ocean Outbreak:

<http://medicine.plosjournals.org/perlserv/?request=get-document&doi=10.1371/journal.pmed.0030263>

Chikungunya information: <http://www.phac-aspc.gc.ca/msds-ftss/msds172e.html>

Source: <http://www.todayonline.com/articles/120065.asp>

27. *May 23, Reuters* — **Iran denies bird flu deaths.** Iran's health minister denied on Tuesday, May 23, that two siblings had died of bird flu, a day after a medical official said they had tested positive for the virus. If bird flu were confirmed as the cause of death, the cases would be the first human deaths from the virus in Iran, which first detected it in birds in February. It has killed people in neighboring Turkey, Iraq and Azerbaijan. On Monday, May 22, an Iranian medical official told Reuters that the 41-year-old man and his 26-year-old sister from the northwestern city of Kermanshah had tested positive for the H5N1 strain of avian influenza that has killed 123 people around the world. Iranian officials also said on Monday that they were sending samples for testing to international laboratories, but on Tuesday the relevant parties had not received them. The two siblings were among five members of a family who became sick. Surviving relatives were in hospital and one was dangerously ill.

Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=worldNews&storyID=2006-05-23T141051Z_01_HKG128373_RTRUKOC_0_UK-BIRDFLU.xml&archived=False

[[Return to top](#)]

Government Sector

28. *May 23, Associated Press* — **Initial tests negative on suspicious powder at Virginia customs facility.** Initial tests have come back negative on a white powder that forced a U.S. Customs and Border Protection facility in Springfield, VA, to be evacuated on Monday, May 22. Customs and Border Protection spokesperson Kelly Kundt says tests revealed that dusts and crumbs were inside the envelope. However, no information was released about where the letter originated or where it was being sent.

Source: <http://www.wjla.com/news/stories/0506/330111.html>

[[Return to top](#)]

Emergency Services Sector

29. *May 23, Seattle Post-Intelligencer* — **Two coordinated terrorism response drills conducted in Puget Sound, WA.** Mock terrorist violence swept across the Puget Sound, WA, area Tuesday, May 23, in an exercise designed to hone the skills of 24 federal, state and local agencies to respond to the real thing. For the past week, the FBI's Washington Joint Analytic

Center has been issuing alarming (albeit bogus) intelligence bulletins to the agencies participating in Tuesday's war games at the Port of Tacoma, according Tom Coyle of the Navy's Center for Asymmetric Warfare. The exercise was coordinated with another drill called "Evergreen Sentry," which calls for detonation of a mock dirty bomb on industrial property at the Port of Everett. The Washington National Guard's Task Force FALCON, which specializes in responding to weapons of mass destruction, was the primary player in the simulation.

Source: http://seattlepi.nwsourc.com/local/271238_terror23.html

30. *May 22, Kansas City Kansan* — **Kansas hosts first responder training for terrorist incidents and major disasters.** Thanks to a collaborative effort of the University of Kansas Medical Center, Kansas City Kansas Community College and Rescue Training Associates of Pompano Beach, FL, approximately 200 first responders were given a wealth of training drills last week. More than two dozen rescue training instructors from Florida, North Carolina, Connecticut, Oklahoma and Kansas spent the week conducting a series of simulated disaster training drills in response to terrorist incidents and major disasters. Federally funded, the training was offered in five tracks: disaster medicine, law enforcement, fire technical rescue, command, and community. Law enforcement officers were put through a simulated hostage drill in which terrorists had placed booby traps and bombs. Fire technical rescue participants crawled into smoking confined areas to treat and rescue the injured. Yet others learned how to cut through metal and concrete to get to patients. Classroom instruction includes being prepared for biologic agents such as smallpox and anthrax being used as weapons; community preparedness for health providers; and even instruction on how to save the lives of dogs specially trained for disasters.

Source: http://www.kansascitykansan.com/articles/2006/05/22/news/new_s1.txt

31. *May 22, American Red Cross* — **Preparedness report released from American Red Cross, New York University.** A report was released by the American Red Cross in Greater New York and New York University's Center for Catastrophe Preparedness & Response, entitled "How Prepared Are We, New York?" This report summarizes the results of a New York City-wide survey indicating that while most New York residents have taken important preparedness actions, there is still more work to be done.

Report: http://www.nyredcross.org/media/81_NYU_Red_Cross_Preparednes_s_Report.pdf

Source: <http://www.nyredcross.org/page.php/prmID/416>

32. *May 22, Contra Costa Times (CA)* — **Volunteer radio operators to monitor AM frequency for crisis communications in California city.** Emergency communication likely will become a key focus of an ambitious Tri-Valley, CA, disaster preparation and recovery plan in the coming weeks, and grass-roots efforts to meet the need are expanding nation-wide. Amateur, volunteer radio operators could play a major part in an expanded emergency-preparedness system. Tri-Valley disaster planners are examining how to improve that communication because public agencies use a variety of radio frequencies and systems. As part of that, San Ramon plans to install its own emergency advisory radio system, an AM broadcast station that would cover the entire city and one to two miles beyond its borders to keep residents updated in case of a disaster. The plan is for every fire station, hospital and emergency operations center to have the system. Similar planning is expanding throughout the state and nationally. Groups that have organized teams of users of small hand-held, battery-powered walkie-talkies or family radio service radios are linking up to form an even more wide-reaching emergency network.

Although amateur and volunteer, the participants have uniform training and methods, and they monitor the same frequencies, which are designated for various uses.

Source: <http://www.contracostatimes.com/mld/cctimes/living/education /14638508.htm>

[[Return to top](#)]

Information Technology and Telecommunications Sector

33. *May 23, BBC (United Kingdom)* — **Web inventor warns against two-tier Internet.** The Web should remain neutral and resist attempts to fragment it into different services, Web inventor Tim Berners-Lee has said. Recent attempts in the U.S. to try to charge for different levels of online access Web were not "part of the Internet model," he said. The open Internet model, backed by Berners-Lee and the World Wide Web Consortium, is based on the concept of network neutrality, where everyone has the same level of access to the Web and that all data moving around the Web is treated equally. But some telecom companies in the U.S. do not agree. They would like to implement a two-tier system, where data from companies or institutions that can pay are given priority over those that cannot. The Internet community believes this threatens the open model of the Internet as broadband providers will become gatekeepers to the Web's content.

Source: <http://news.bbc.co.uk/1/hi/technology/5009250.stm>

34. *May 22, Security Focus* — **Skype URI handling remote file download vulnerability.** Skype is prone to an arbitrary file download vulnerability. This issue is due to improper Skype URI handling. Analysis: This issue allows remote attackers to transfer files from one Skype user to another, provided the recipient user has previously approved downloads. By exploiting this issue, attackers may retrieve an arbitrary file from the victim user's computer.

Affected products: <http://www.securityfocus.com/bid/18038/info>

Solution: The vendor has released an advisory along with fixes to address this issue:

<http://www.skype.com/security/skype-sb-2006-001.html>

Source: <http://www.securityfocus.com/bid/18038/discuss>

35. *May 22, FrSIRT* — **Linux kernel "snmp_trap_decode()" remote memory corruption vulnerability.** A vulnerability has been identified in Linux kernel, which could be exploited by remote attackers to cause a denial-of-service. This flaw is due to a memory corruption error in the "snmp_trap_decode()" [ipv4/netfilter/ip_nat_snmp_basic.c] function when allocating the ID and the address, which could be exploited by remote attackers to crash a vulnerable system where the "ip_nat_snmp_basic" module is loaded and traffic on port 161 or 162 is NATed.

Affected products: Linux kernel version 2.6.16.17 and prior.

Solution: Upgrade to Linux kernel version 2.6.16.18: <http://www.kernel.org/>

Source: <http://www.frstirt.com/english/advisories/2006/1916>

36. *May 22, InfoWorld* — **Microsoft: Word zero-day patch by June.** Microsoft plans to patch a newly discovered hole in Microsoft Word in its next monthly patch update, and may release a rare "out of cycle" patch to address the hole, a company spokesperson said. Microsoft's Security Research Center is analyzing the previously unknown vulnerability, which affects Microsoft Word XP and Word 2003 and is already being linked to targeted Internet attacks on government

agencies in the U.S. and European Union, as well as U.S. government defense contractors. Anti-virus firms warned of the unknown Word hole on Friday, May 19, after attacks were first detected. Microsoft is completing development of a security update for Microsoft Word that addresses the vulnerability. The fix is being tested and could be released on Tuesday, June 13, with the company's scheduled monthly patch release, or sooner.

Source: http://www.infoworld.com/article/06/05/22/78575_HNword0dayjune1.html

37. **May 21, SecuriTeam — Apple Safari JavaScript denial-of-service vulnerability.** A recent vulnerability has been discovered with Apple Safari Web browser. Analysis: Safari is a Web browser developed by Apple Computer, Inc. and available as part of Mac OS X. It was included as the default browser in Mac OS X v10.3 (Panther) and is the only browser bundled with Mac OS X v10.4 (Tiger). An Infinite loop in JavaScript may cause a denial-of-service condition on vulnerable Safari browser. Solution: Disable JavaScript.

Source: <http://www.securiteam.com/unixfocus/5CP0P0AIKI.html>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is currently researching a zero-day vulnerability in Microsoft Word. In order for this exploit to be carried out, a user must first open a malicious Word document attached to an email or otherwise provided to them by an attacker. When the document is opened, malicious code is installed on the user's machine. The exploit then attempts to connect to a remote host. US-CERT and Microsoft will continue to investigate the public reports to help provide additional guidance as necessary. There is currently no patch available for this vulnerability.

For more information please review the following:

TA06-139A Microsoft Word Vulnerability:

<http://www.us-cert.gov/cas/techalerts/TA06-139A.html>

VU#446012 Microsoft Word buffer overflow: <http://www.kb.cert.org/vuls/id/446012>

Cyber Security Tip: <http://www.us-cert.gov/cas/tips/ST04-010.html>

Microsoft Security Advisory (919637):

<http://www.microsoft.com/technet/security/advisory/919637.mspx#EAF>

US-CERT recommends the following actions to mitigate the security risks:

Install anti-virus software, and keep its virus signature files up to date

Block executable and unknown file types at the email gateway

US-CERT strongly encourages Federal Agencies to educate their user base and constituency about the risk of opening unknown attachments from unknown sources even if sent by a known and trusted source.

We will continue to update current activity as more information becomes available.

PHISHING SCAMS

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

| | |
|----------------------------|---|
| Top 10 Target Ports | 1026 (win-rpc), 6881 (bittorrent), 25 (smtp), 38566 (----), 445 (microsoft-ds), 12106 (----), 7200 (fodms), 50497 (----), 49200 (----), 41170 (----) Source: http://isc.incidents.org/top10.html ; Internet Storm Center |
|----------------------------|---|

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

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

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

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

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

General Sector

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.