



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 09 April 2004

Current Nationwide Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports that two explosions followed by fire rocked a gasoline refinery in western New Mexico Thursday seriously injuring four people (See item [2](#))
- CNN reports that the FBI is investigating how an incendiary device ended up in a restroom at Hartsfield–Jackson International Airport in Atlanta Wednesday. (See item [16](#))
- CNET News.com reports that Cisco Systems warned customers on Wednesday, April 7, that a preset username and password coded into the company's Wireless LAN Solution Engine (WLSE) and Hosting Solution Engine (HSE) could give attackers complete control of the devices. (See item [30](#))
- The US–CERT has issued Technical Cyber Security Alert TA04–099A: Vulnerability in Internet Explorer ITS Protocol Handler. (See item [32](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web 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://esisac.com>]

1. *April 08, Reuters* — **Government sees record U.S. summer gas prices.** U.S. consumers can expect to pay a record average \$1.76 a gallon for gasoline during this summer's busy driving season, 20 cents more than last year, and the national pump price could top \$1.80, the

government said on Thursday, April 8. "High crude oil costs, strong gasoline demand, low gasoline inventories and more stringent gasoline specifications this year have increased gasoline supply costs and retail prices to high levels well before the peak driving season," the Energy Information Administration (EIA) said in its annual summer forecast. **The Department of Energy's analytical arm warned that the U.S. gasoline supply system is "vulnerable" to severe price spikes if major refinery or pipeline outages occur. America's motor gasoline inventories are currently at one of the lowest levels seen for this time of year in almost three decades, according to EIA.** Gasoline stocks stood at 200 million barrels at the beginning of April, the second-lowest level in 30 years. By the end of the summer driving season in September, inventories are projected to be 201 million barrels, which is within the normal range, the agency said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A60713-2004Apr 8.html>

- 2. *April 08, Associated Press* — Four critically injured in refinery blast. Two explosions followed by fire rocked a gasoline refinery Thursday, April 8, seriously injuring four people, officials said.** Smoke billowed from the east side of the Giant Industries refinery about 15 miles east of Gallup in western New Mexico as rescue crews converged on the scene. Firefighters quickly contained the blaze. **State police Lt. Jimmy Glascock said it was unclear what caused the first explosion, but the second occurred when a piece of equipment used to make high-octane fuel malfunctioned.** Donelle Chandler, a spokeswoman for Giant Industries in Scottsdale, AZ, did not have any immediate comment on the explosion except to say company officials were looking into it. Glascock said a nearby propane pipeline was vented after the explosions and the gas burned off to prevent more explosions.

Source: <http://www.cnn.com/2004/US/Southwest/04/08/refinery.explosion.ap/index.html>

- 3. *April 07, Reuters* — Illinois lets company reopen crude unit. Illinois will allow ConocoPhillips to reopen a crude unit at a currently closed refinery to avert a gasoline crunch this summer. Illinois Governor Rod Blagojevich instructed the state's environmental regulators on Tuesday, April 7, to authorize a construction permit for the crude unit at the Hartford refinery, which used to run at 70,000 barrels per day. The unit should be in working order in about seven days, the governor said in a statement. "The bottom line is that gasoline shortages means increased gasoline prices," the governor said in statement. A Conoco official said the opening of the crude unit will offset problems at Conoco's adjacent Wood River refinery.**

Source: http://biz.yahoo.com/rc/040407/energy_conoco_illinois_1.html

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

Chemical Sector

- 4. *April 08, WTAP-TV (WV)* — Chemical discharge. Dupont is investigating an early morning release of a substance from the Washington Works plant in West Virginia. The substance, called fluorinated ethylene propylene, was discharged after a rupture of a relief line shortly after 4 a.m. Wednesday, April 7.** Some of the fine, white powder spilled into the Ohio River, and later, part of it could be seen as far south as the Belleville, WV, locks and dam. "We sent crews, cleaning up that material from the locks and dam," says Robin Ollis, External Affairs Manager. "We don't have any information that it's gone any further than that

dam." The accident forced the shutdown at the plant unit where the product comes from, but Ollis says it's been "business as usual" throughout the rest of the complex.

Source: <http://www.wtap.com/news/headlines/669827.html>

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

Defense Industrial Base Sector

5. *April 08, The Fayetteville Observer (NC)* — **Schoomaker explains Army goals.** The Army will undergo changes that will provide more stability for soldiers and their families, the Army's top general said Wednesday, April 7, at Fort Bragg, NC. Gen. Peter J. Schoomaker, the Army chief of staff, is leading the charge to make the Army more agile and lethal in a process known as "transformation." The plan calls for the Army to increase its number of combat brigades from 33 to 45. The small units are more deployable and provide more units to deploy. **Also, in hopes of saving money and keeping experienced combat veterans with their units, Schoomaker said, soldiers will have longer tours. Under a policy called "homesteading," soldiers will remain at a post for up to seven years. Most officers change commands and duty stations every two or three years.** Schoomaker said the Army spends almost a billion dollars moving soldiers from one duty station to another, with 296,000 soldiers being moved last year alone. By staying in place longer, Schoomaker said, units are more cohesive and more combat ready. Schoomaker has been working to transform the Army since he took over as chief of staff last year.

Source: <http://www.fayettevillenc.com/story.php?Template=military&Story=6273519>

6. *April 08, Associated Press* — **Investigators look into tampering of gas meter at National Guard armory. Someone used a rubber hose to connect a gas meter to an electrical conduit at a National Guard armory with the apparent intention of damaging the building, police said** Thursday, April 8. The tampering, which caused no damage, was discovered by a New York State Electric and Gas employee March 30. Police don't know when the meter was vandalized. "The way it was set up, if anything, you might have had a fire outside the building," said Brian Donnelly, chief of police in Olean, about 60 miles south of Buffalo, NY. "The gas meter had a valve on the top and they put a hose on the valve and ran it up to an electrical conduit and then put it up into the conduit," Donnelly said. "The gas was turned on but apparently it just vented and there was never a problem with it." The meter is about 10 feet from the side of the armory, which houses Company C of the 1st Battalion, 127th Armored Division of the National Guard.

Source: <http://www.newsday.com/news/local/wire/ny-bc-ny-brf--armorytamperi0408apr08,0,2896508.story?coll=ny-ap-regional-wire>

7. *April 07, Associated Press* — **New command renews Navy focus on hunting submarines.** The Navy is creating a command to strengthen its ability to hunt submarines, including quiet diesel-electric subs that patrol shallow waters and could pose a threat to U.S. forces in areas of conflict. The Fleet Antisubmarine Warfare Command (ASW) opens with a ceremony Thursday, April 8, in San Diego, CA. The command will be based there but will report to Fleet Forces Command on the other side of the country, in Norfolk, VA. **The Navy is renewing its focus on ASW (not a major focus after the Cold War), because many countries, including North Korea, India, China and Iran, have diesel submarines that stay close to beaches and are**

very quiet when they run on electric power underwater. ASW involves many platforms, including surface ships, airplanes and submarines. Historically, those communities within the Navy did ASW in an individual fashion. The new command integrates those elements, bringing together people from throughout the Navy who have ASW expertise. The intent is to make ASW more efficient and effective by identifying and fixing witnesses, bolstering strengths and eliminating duplication of efforts, said Bob Brandhuber, director of antisubmarine warfare improvement for the Navy's Pacific Fleet.

Source: http://www.mercurynews.com/mld/mercurynews/news/local/837868_2.htm

[[Return to top](#)]

Banking and Finance Sector

8. *April 08, Honolulu Advertiser* — **Scam role puts man in prison.** A 67-year-old Honolulu, HI, man has been sentenced to two years in federal prison for his role in an Internet bank fraud scheme that has been associated with Nigerian con artists. Federal prosecutors believe that Yoshiaki Fujimoto is the first person convicted in Hawaii for his involvement in the Nigerian scam. Fujimoto was contacted by a Nigerian in the summer of 2002 who offered him a large sum through a third person, according to court documents. **Fujimoto was sent a \$245,000 check, payable to himself that was drawn on a New York bank. However, prosecutors said the check was stolen, "washed" clean and then made payable to Fujimoto. They said he attempted to deposit the check in his Territorial Savings account on July 19, 2002, but was told by a bank official that the check was fraudulent and part of a scam.** Fujimoto ignored the warning and used the check to open an account at another bank, prosecutors said. He then wired \$100,000 to accounts in New York and Indonesia, prosecutors said. Assistant U.S. Attorney Michael Seabright said it's nearly impossible to retrieve the money once it is wired to someone out of state.

Source: http://the.honoluluadvertiser.com/article/2004/Apr/08/ln/ln1_9a.html

9. *April 08, The Herald (WA)* — **Suspected identity theft ring broken. Sheriff's deputies and federal agents say they may have broken up a major identity theft ring when they arrested three people at a Bothell, WA-area apartment, confiscated bags of stolen mail and found 40 pieces of stolen or false identification. Found were passports and the identification of people from California, Oregon, Colorado and Washington, court papers say. The identifications of two FBI agents also were found, documents say.** The three suspects appeared Wednesday, April 7, in Everett District Court. Scott Christopher Moughton and Thomas F. Sproul were held on \$250,000 bail each. Elizabeth R. Hoefert, Moughton's girlfriend, was held on \$2,000 bail. The three were arrested Tuesday, April 6, after deputies nabbed another two men they believed were involved in mail thefts at an apartment complex in the Thrasher's Corner area. The two told deputies they had been in Moughton's apartment and watched him make an identification card on his computer. The men said Moughton had a laptop computer, printers and other equipment to make checks, Social Security cards and identifications. **One of the men said up to 40 people daily brought Moughton stolen mail, and he particularly liked bank cards, court papers say.**

Source: <http://www.heraldnet.com/Stories/04/4/8/18452525.cfm>

10.

April 08, Click2Houston.com — **Company warns customers about possible identity theft.** Officials and a company owner said there is a chance some Montgomery County, TX, residents had their financial secrets stolen over the weekend. **Police said thieves stole computer equipment -- including hard drives, servers, monitors and other items -- from First Option Financial, May Realty, Farmers Insurance, LPL Financial and Stewart Title, located in an office building. The stolen information included Social Security and credit card numbers, and bank account information of thousands of clients.** Investigators said the business burglaries were the work of identity thieves. While the stolen information has not turned into an identity theft, the possibility does exist for anyone who has dealt with mentioned companies over the past three years, according to First Option Financial Services spokesperson John Caballero.

Source: <http://www.click2houston.com/money/2985156/detail.html>

11. *April 07, The Dominion Post (NZ)* — **Banking scam hits National customers. National Bank in New Zealand is the latest bank to be hit by an internet-based scam asking customers to divulge confidential password and login details.** Called "official notice," the e-mail tells customers online banking details have been lost due to database problems. Recipients are then directed to another page and asked for their customer identification number and password. The bank's corporate communications general manager, Cynthia Brophy, said it had alerted police and warned customers on its Website not to reply to the e-mail. Brophy said that to the bank's knowledge, no suspicious transactions had occurred since the bogus e-mails appeared on Monday, April 5. **The e-mail was thought to originate in the United States.**

Source: <http://www.stuff.co.nz/stuff/0,2106,2868076a11,00.html>

12. *April 07, The Boston Channel* — **Credit card mailing is scam in disguise.** A new identity theft scam is particularly alarming because at first glance it looks like official information from your credit card company, and says your card is going to cost more money if you don't act immediately. **The information comes in an envelope that reads "Customer Care Center," but there is no company name or logo. Inside the mailing it says, "Notice of change in terms to your card agreement."** Among the changes outlined is an increase in the "annual percentage rate of 27.99%." It then tells consumers that they can chose not to accept the agreement by using the "non-acceptance instructions." **Under the non-acceptance instructions the company says you "must notify us in writing" including your name, address and credit card number.** Susan Wornick, a consumer reporter, said the most recent mailing is one of the more clever attempts to get personal information and credit card numbers.

Source: <http://www.thebostonchannel.com/buyerbeware/2983016/detail.html>

13. *April 05, Austin Business Journal* — **Banks, law enforcers set up anti-fraud network.** **Several Texas financial organizations have joined with law enforcement agencies to fight fraud and identity theft, which costs businesses and consumers millions of dollars every year. The banking network will be supported by the Texas Attorney General's Office, the Texas Department of Public Safety and the FBI.** The SouthWestern Automated Clearing House Association, already operating a fraud alert system for its members, will manage what's called the Loss Avoidance Alert System. The Independent Bankers Association of Texas, the Texas Credit Union League, the Texas Savings Association and the Texas Savings and Community Bankers Association will participate in the network, which will notify local financial institutions and law enforcement agencies about suspected illegal activity.

Participating organizations can post notices about forgeries, counterfeit checks, lost checks and other problems. Network members can research past abusers to identify patterns of behavior.
Source: http://austin.bizjournals.com/austin/stories/2004/04/05/daily4.html?jst=b_in_hl

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

Transportation Sector

14. *April 08, Washington Times* — **Senators say U.S. slow to arm pilots.** The federal government is stalling the process to arm airline pilots, according to lawmakers pushing new legislation to jump-start the program created in 2002. **Senators Jim Bunning, Kentucky Republican, and Barbara Boxer, California Democrat, introduced the bill before the Easter recess to force the Transportation Security Administration (TSA) to implement the Federal Flight Deck Officer program the way Congress intended.** Only two percent of 100,000 eligible pilots have been trained to carry guns. They are then forced to carry the weapons in a lockbox, unless they are behind a locked cabin door, and are forbidden from carrying weapons on international flights, rules pilots have said undermine the program. **The bill requires the government to immediately deputize as air marshals any pilots with military or law enforcement background who are already trained to carry weapons.** Those already trained would have 180 days to go through additional government training, and any new volunteers would have to be trained within 90 days. Pilots would be allowed to carry guns on international flights, and to carry guns holstered instead of in lockboxes.

Source: <http://washingtontimes.com/national/20040407-111335-1734r.htm>

15. *April 08, Newhouse News Service* — **New Jersey's transit safety plan. New Jersey's \$102 million transportation-security plan provides for surveillance cameras on bridges, increased police patrols on trains, and extra bomb-sniffing dogs,** during a legislative budget hearing April 6. Homeland security measures, many of which are already in place, became a focal point of the hearing when several members of the Assembly Budget Committee expressed concerns about last month's terrorist bombings of commuter trains in Madrid and asked what was being done to prevent such attacks here. "Most of our ability to respond to an incident like Madrid flows from systems beefed up on the heels of 9/11," Transportation Commissioner Jack Lettiere said. "Before that, we had nothing in place virtually. It was a learning experience from day one." Since then, Lettiere said, the state has done everything possible to keep its highways and mass transit systems safe.

Source: http://www.nj.com/news/jjournal/index.ssf?base/news-1/10814_15803290320.xml

16. *April 07, CNN* — **Incendiary device found in Atlanta airport.** The FBI launched an investigation Wednesday, April 7, into how an incendiary device ended up in a restroom at Hartsfield-Jackson International Airport, one of the world's busiest airports. The discovery shortly forced the evacuation of a small area of the airport. The FBI said its Joint Terrorism Task Force was investigating who might have placed the device in the airport. **The FBI described the device as "similar to a military trip flare containing highly flammable substance."** "This device could have caused very serious injury to anyone handling or tampering with the device," the FBI statement said. The device was found shortly in a men's restroom in the airport atrium, outside an area where security checks are performed, an airline security source said. Using a robot, police moved the device to a secure area and conducted a

controlled detonation, disabling the device.

Source: <http://www.cnn.com/2004/TRAVEL/04/07/suspicious.device/>

17. April 06, Trucker — **TSA extends fingerprint deadline. As the deadline for the fingerprint-based background checks for hazmat drivers was approaching, the Department of Homeland Security's Transportation Security Administration (TSA) formally stretched its deadline to January 31, 2005.** The deadline had been April 1 of this year. That was the date for states to begin collecting fingerprints and providing them to the FBI. A TSA release stated that "TSA is providing states additional time to make the significant changes to their existing commercial driver safety and testing programs." **The plan entails making background checks on the nation's estimated 3.5 million hazmat drivers to determine potential terrorist activity or terrorist connections.** Last May TSA published its Interim Final Rule on implementing background checks including the fingerprinting. The checks were mandated by the USA Patriot Act and the Safe Explosives Act. The act gave TSA the responsibility for collecting and transmitting fingerprints and other data to the FBI, but the states will actually be collecting the fingerprints and administering the hazmat endorsements, whereas TSA will have the say—so over who is a threat and who is ineligible for a hazmat endorsement. .

Source: http://www.thetrucker.com/stories/04_04/0406_fingerprint_deadline.html

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

18. April 08, Dow Jones Newswires — **Lawmakers oppose plan to import Canadian cattle.** Seven U.S. senators sent a letter to Agriculture Secretary Ann Veneman on Wednesday, April 7, urging her to withdraw a proposal that could allow live cattle shipments from Canada to the United States as early as this spring. Wednesday was the last day for public comment on the proposal to reopen the border to cattle younger than 30 months of age. The U.S. border was closed to Canadian cattle last May after a case of mad cow disease was found on an Alberta farm. Some beef exports resumed last fall. Cross-border cattle shipments have remained banned following the discovery of mad cow disease in a Washington state dairy cow that originated in Alberta. **Senator Patty Murray, D-WA, joined senators from six other states in urging the U.S. Department of Agriculture (USDA) to drop the proposal, which would list Canada as a country with "minimal risk" for mad cow disease. "While USDA appears determined to significantly increase its mad cow testing, we are concerned that you are not requiring Canada to meet the same high standards," the senators said in the letter.**

Source: http://www.agprofessional.com/show_story.php?id=24455

19. April 08, Nebraska Ag Connection — **Tool helps track livestock diseases. A University of Nebraska-developed computer-based system could help track various livestock diseases,**

whether domestic, foreign, or the result of bioterrorism. It's among the latest tools developed by remote sensing and geographic information specialists at the university's Center for Advanced Land Management Information Technologies (CALMIT) to help state and federal agencies anticipate, manage, and respond to diseases, natural disasters, and potential bioterrorism. **The system tracks and monitors animals based on species, location, number, proximity to veterinarians, outbreaks, and susceptibility to diseases.**

Source: <http://www.nebraskaagconnection.com/story-state.cfm?Id=201&y r=2004>

20. *April 07, Oster Dow Jones Commodity News* — **Safety rules for BSE will cost millions.** The annual cost to U.S. cattle producers and beef processors of conforming to several new rules to guard against the spread of bovine spongiform encephalopathy (BSE) will range from \$110.3 million to \$149.1 million, according to a U.S. Department of Agriculture (USDA) report released April 8. In response to the December discovery of a BSE-infected cow in Washington state, the USDA announced new regulations that ban meat from non-ambulatory, or "downer" animals, from the human food supply, expand the types of bovine tissue considered to be a risk of carrying BSE, and further restrict advanced meat recovery technology to scrape meat from carcass bones. The report, issued by USDA's Food Safety and Inspection Service (FSIS), said the new rules are necessary because, in part, they "provide greater assurances to both domestic and foreign consumers that the U.S. beef supply is safe." **The FSIS, in breaking down the costs for the separate rules, said the new prohibition on downer cattle will cost producers about \$36 million per year, while the economic impact of new restriction on BSE specified risk materials, commonly called SRMs, will be \$99.9 million to \$136.6 million.**

Source: http://www.agprofessional.com/show_story.php?id=24441

21. *April 07, Agriculture Online* — **Farmers developing new tools to fight soybean rust.** Government agencies and agribusinesses this week stepped up efforts to arm U.S. farmers with tools to fight Asian soybean rust, the disease that can cut crop yields by half or more. **On Tuesday, April 7, the Environmental Protection Agency (EPA) approved emergency use of the fungicide myclobutanil in South Dakota and Minnesota to treat soybean rust.** "This action will provide farmers some fungicide tools to use should soybean rust ever occur in the United States," EPA representative David Deegan said. "The emergency situation is not in question," he said. EPA also is reviewing several other fungicides for use against soybean rust, Deegan said. **EPA's action is prompted not only by the potentially severe economic impact of the disease, but also because Asian soybean rust has been identified by the U.S. government as a possible biological weapon,** Deegan said. Soybean rust, which originated in Asia and Australia, is moving northward from South America where it was first reported in 2001. Southern U.S. conditions are "very susceptible" to soybean rust, Morris Bonde, a soybean rust researcher said. **"Sentinel plots" have been established in the South to help provide an early warning.**

Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=topStoryDetail_ANewsindex.html_51565_1

[[Return to top](#)]

Food Sector

22.

April 08, Herald (United Kingdom) — **UN warns that grain stocks are becoming low.** The Food and Agricultural Organization (FAO) of the United Nations has issued a warning that world cereal stocks are approaching a dangerously low level. **According to the FAO's report, Food Outlook, global stocks of grain are set to fall by 18 percent, or 89 million tons, by the end of the 2003/04 crop season.** The decline is largely due to a fall in production in China, but there have also been substantial drops in India, Russia, Ukraine, and the European Union, chiefly as a result of a severe drought last summer. However, the FAO report anticipates that world cereal production in 2004 will increase to 2130 million tons, which is two percent higher than last year. The bulk of the increase is expected to be wheat, but there could also be a significant rise in rice production. **Much will depend on the weather in the coming months. The western states of the U.S. are experiencing drought conditions, with the result that wheat crops have suffered.**

Source: <http://www.theherald.co.uk/business/13600.html>

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

Water Sector

23. *April 07, WJRT (Michigan)* — Michigan water supply threatened. U.S. intelligence learned a little over two weeks ago that Michigan's water supplies could be a target of terrorism. The FBI's Bill Kowalski and Genesee County Drain Commissioner Jeff Wright have confirmed the alert. Security was heightened statewide when Michigan's homeland security director received a bulletin from Washington's intelligence agencies. Directives were then filtered from Michigan State Police to local jurisdictions. Police at that point were told to keep a lookout at local water stations. **The threat, which wasn't specific, lasted two days a little over two weeks ago.**

Source: http://abclocal.go.com/wjrt/news/040704_NW_da_water.html

24. *April 07, Reuters* — D.C. lead woes prompt scrutiny of federal rules. Chronic problems with high levels of lead in Washington D.C.'s water supply are prompting scrutiny of water regulation at the national level, members of Congress and the Environmental Protection Agency said on Wednesday, April 7. **Senator James Jeffords, a Vermont independent, told a Senate hearing he planned to introduce a bill within days that would require testing for lead in water systems across the country, eliminate lead service lines and pipes, and prohibit lead in plumbing fixtures.** The bill would also require immediate notification of all homes with elevated lead test results and require public water systems to provide in-home filters where lead is a problem. The EPA requires utilities to notify the public and in some cases replace lead pipes if lead rises to more than 15 parts per billion in water supplies, but lawmakers at the hearing said the experience of residents of the nation's capital city highlighted regulatory shortcomings. Regular tests of D.C. water in 2002 revealed elevated lead levels in an unexpectedly high proportion of test samples, and a much larger sampling last summer showed thousands of homes above the 15 parts per billion level. Residents say they were sent only a proforma letter about the results with no follow-up from city health authorities.

Source: <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=4779800>

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

Public Health Sector

25. *April 08, Seattle Times* — **Hundreds might have been exposed to measles. Seven children from King and Snohomish counties Washington have confirmed or probable cases of red measles and may have exposed hundreds of people in 21 public places.** All of the children were recently adopted from China and came to the U.S. with their new families on March 26. Health officials are urging people who have been in any of the locations at certain times and have not been immunized, or are unsure of their immunization status, to contact their doctors. Measles is highly contagious but uncommon in the United States. It can have serious complications and is sometimes fatal. **U.S. Centers for Disease Control and Prevention officials are investigating whether two of the children exposed airline passengers on their trips.** Several flights were involved, health authorities said.

Source: http://seattletimes.nwsourc.com/html/localnews/2001898367_m easles08m.html

26. *April 08, Chicago Tribune* — **Bioterror detectors go high-tech.** Government analysts have begun scanning the U.S. daily for the first signs of a bioterror attack by monitoring enormous databases that include over-the-counter drug sales and common ailments reported in hospital emergency rooms. The experimental high-tech program is part of a new effort to develop early warning systems for imminent public health crises and is analogous to those that scan the skies for a missile attack. **BioSense, run by the U.S. Centers for Disease Control and Prevention (CDC), quietly began operating late last year. It is designed to pick up signals of potential health emergencies as close to the onset as possible. Instead of relying on confirmed medical diagnoses, the program focuses on symptoms such as fever, rash, diarrhea, or nausea, searching for unusual patterns or clusters.** Eventually, the system will scan a wide variety of information sources for signs of possible disease outbreaks, from school absenteeism rates to sharp spikes in doctors' visits. **The program joins BioWatch, a network of air sensors in 31 cities that are sniffing for toxic substances, and a new CDC program to electronically track illness outbreaks across the country.**

Source: http://www.chicagotribune.com/technology/chi-0404080262apr08_1.3499621.story?coll=chi-techtopheds-hed

27. *April 08, Associated Press* — **World to eradicate polio by 2005. The world is likely to eradicate polio by next year, making it the second known disease after smallpox to be wiped out by mankind, the U.S. health secretary said Thursday, April 8.** "We're on the precipice of accomplishing it," the secretary of Health and Human Services, Tommy Thompson, told a news conference after what he said was an encouraging day of hearing ambitious plans by Indian officials and volunteers to make sure all children under 5 are immunized. **"We're probably down to the last 1,000 cases, probably the most difficult to eradicate," he said.** The cases are in India, Pakistan, Afghanistan, Egypt, Nigeria, and Niger.

Source: <http://www.mlive.com/newsflash/health/index.ssf?/base/international-1/1081433341298030.xml>

[[Return to top](#)]

Government Sector

Nothing to report.

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

Emergency Services Sector

28. *April 08, Nbc5i.com (TX)* — **City's warning system not yet up to speed. A new \$3 million outdoor warning system in Fort Worth, TX, is getting mixed reviews. City leaders tested the warning system for the first time Wednesday, April 7, and not all of the sirens went off.** They say the problems will be fixed, and the sirens that worked still outnumber the total sirens with the old warning system. "We already have a better system than what we had before. Now the system is not in any way complete and there is still some additional work that needs to be done," said Juan Ortiz, Emergency Management Office. The city will not make the final payment on the system until it works perfectly for 30 days straight.

Source: <http://www.nbc5i.com/news/2985601/detail.html>

29. *April 07, Federal Computer Week* — **DHS helps localities use tech.** In the next several weeks, the Department of Homeland Security (DHS) will unveil a new initiative to implement technologies and systems into local communities and regions. With strong cooperation from local and regional jurisdictions, DHS officials will help the transition and integration of advanced technologies into those communities from a bottom-up approach rather than a top-down approach, said Nancy Suski, director of emergency preparedness and response within DHS's Science and Technology Directorate. Safe Cities is different from other programs because these are technologies that have already been tested. "It's really ready for an operational testing in real-world settings to become a part of the operational infrastructure. It looks at the human interfaces that are required" and how it contributes to the decision-making process, Suski said. It's also not technology specific. **"I work very closely with my other portfolio managers that are helping me on just the bio threat or just the [chemical] threat or the [radiation] threat," she added. "How do all those systems that each of those portfolios are working on come together into a construct that really is going to help a community be protected and be ready to respond in the event a catastrophe actually occurred."**

Source: <http://www.fcw.com/geb/articles/2004/0405/web-safecities-04-07-04.asp>

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

Information and Telecommunications Sector

30. *April 08, CNET News.com* — **Cisco bug could put hackers in driver's seat.** Cisco Systems warned customers on Wednesday, April 7, that a preset username and password coded into the company's Wireless LAN Solution Engine (WLSE) and Hosting Solution Engine (HSE) could give attackers complete control of the devices. WLSE has security features that can detect unauthorized or rogue access points. **If an attacker is able to control this management tool, he or she could hide the presence of a rogue access point or change the radio frequency plan,** potentially causing systemwide outages. The HSE allows authorized users to remotely monitor, activate and configure services and devices, even through firewalls. **The security hole could allow attackers who gain access to the device to use it as a launching platform to**

redirect traffic coming into or out of the data center. The vulnerability affects WLSE versions 2.0, 2.0.2 and 2.5 and HSE versions 1.7 through 1.7.3. Patches are available on the Cisco Website: http://www.cisco.com/en/US/products/products_security_advisory09186a00802119c8.shtml
Source: http://news.com.com/2100-1039_3-5187233.html?tag=nefd.top

31. *April 08, CNET News.com* — **NetSky attacks target file-sharing networks.** The main Website of file-sharing network eDonkey was knocked offline this week following an attack from NetSky. Earlier this week, the Kazaa and eDonkey sites, as well as three other file-sharing sites, were bracing for a distributed denial-of-service (DDoS) attack expected to be launched by variants of the NetSky worm. **NetSky.Q, which first appeared March 29, is designed to attack certain Websites that distribute file-sharing clients, as well as sites that distribute hacking and cracking tools. The attack is scheduled to last at least six days.** Another target, eMule, has also experienced severe disruption and in preparation has mirrored its site to another address. One of the Crack Websites, www.cracks.am, was unavailable, and another, www.crack.st, had been unavailable earlier. Kazaa's Web site seems to be the only one of Netsky's targets to have survived the first day of the attack unscathed.
Source: http://news.com.com/2100-1009_3-5187211.html?tag=nefd.top
32. *April 08, US-CERT* — **Technical Cyber Security Alert TA04-099A: Vulnerability in Internet Explorer ITS Protocol Handler. A cross-domain scripting vulnerability in Microsoft Internet Explorer (IE) could allow an attacker to execute arbitrary code with the privileges of the user running IE.** The attacker could also read and manipulate data on web sites in other domains or zones. Any programs that use the WebBrowser ActiveX control or the IE HTML rendering engine (MSHTML) may be affected by this vulnerability. **Publicly available exploit code exists for this vulnerability.** Currently, there is no complete solution for this vulnerability but information about workarounds is available on the US-CERT Website.
Source: <http://www.us-cert.gov/cas/techalerts/TA04-099A.html>
33. *April 07,* — **Flaw in RealPlayer client could allow remote attack.** RealNetworks Inc. has announced that a flaw in a component of many of its client systems could allow a remote attacker to execute arbitrary code on the user's system. **If an attacker were to exploit the vulnerability successfully, he or she could, minimally, produce a denial of service in the R3T plug-in. It may also be possible for the attacker to execute arbitrary code with the same privileges as the user of the player.** The attacker would have to entice the user to load a malformed file designed to invoke the vulnerability, probably by luring the user to a Website that contains Real media. RealPlayer 8, RealOne Player, RealOne Player v2 for Windows only, RealPlayer 10 Beta, and RealPlayer Enterprise are affected. Additional information available on the Real Website: http://service.real.com/help/faq/security/040406_r3t/en/
Source: <http://www.eweek.com/article2/0.1759.1563018.00.asp>
34. *April 06, CNET News.com* — **Apple releases patches for Jaguar, Panther.** Apple released updates for the Panther and Jaguar versions of Mac OS X that fix security issues in the operating systems' printing, mail and encryption capabilities Monday, April 5, as well as a critical vulnerability in the handling of Web addresses. **The most critical vulnerabilities, in a common Unix library for the extensible markup language (XML), could allow an attacker to execute code on a victim's computer by sending a long address, also known as a Uniform**

Resource Locator, or URL. Apple also fixed two flaws in OpenSSL that made PCs vulnerable to a denial-of-service attack. Apple released little information on the flaws in the Mac OS X's printing capabilities and the system's mail services. Additional information is available on the Apple Website: <http://www.apple.com/support/>
 Source: <http://news.com.com/2100-7355-5185918.html?tag=cd.top>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_NETSKY.P Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 445 (microsoft-ds), 80 (www), 3127 (mydoom), 137 (netbios-ns), 139 (netbios-ssn), 2745 (urbisnet), 1434 (ms-sql-m), 1433 (ms-sql-s), 6129 (dameware) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

35. *April 08, BBC News* — **Abu Sayyaf leader killed. The Philippines' armed forces say they have killed one of the five leading members of the Abu Sayyaf, an armed group of Filipino Muslims notorious for kidnapping hostages.** The army says the man, Hamsiraji Sali, was killed during an exchange of fire with an elite unit who cornered him in a village on the southern island of Basilan. Some other members of the group were also killed and four soldiers wounded. **The U.S. had offered a reward of one million dollars for the capture of Sali who was wanted for his alleged part in kidnapping three Americans in the Philippines nearly three years ago.** Two of the Americans were killed while in captivity. Although the Abu Sayyef's main occupation is kidnapping for ransom, the U.S. says it regards them as terrorists because of their past links with Osama bin Laden.

Source: <http://news.bbc.co.uk/2/hi/asia-pacific/3611577.stm>

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

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Publications](#) – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644

Subscription and Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

Contact DHS/IAIP

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 info@us-cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.