



# Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 21 August 2003

Current Nationwide Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](#)  
[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- PRNewswire reports CSX Transportation's information technology systems experienced significant slowdowns early Wednesday, halting some passenger and freight train traffic, after a computer virus infected the network. (See item [11](#))
- The Associated Press reports a Michigan meat processor has issued a voluntary recall of about 3,600 pounds of fresh beef products that the federal government said were processed under unsanitary conditions. (See item [15](#))
- Microsoft has released "Security Bulletin MS03-032: Cumulative Patch for Internet Explorer (Critical)," and a patch is available on the Microsoft Website. (See item [25](#))
- Microsoft has released "Security Bulletin MS03-033: Unchecked Buffer in MDAC Function Could Enable System Compromise (Important)," and a patch is available on the Microsoft Website. (See item [26](#))
- The Dow Jones Newswire reports that the Sobig.F computer virus, thought to be the fastest-spreading e-mail virus of all time, deposits a Trojan horse that can be used to turn victims' PCs into spam machines. (See item [27](#))

### 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. *August 20, Washington Post* — **U.S. and Canada to control blackout probe. The North American Electric Reliability Council (NERC) was leading the investigation into the blackout last week that affected much of the northeast and midwest United States and Canada. However, the Department of Energy has decided that it will lead the probe. Now, NERC, independent power system operators, and executives from utility companies will pitch in with the government's investigation, which already involves hundreds of officials.** Industry officials said Secretary of Energy Spencer Abraham's decision to absorb the NERC investigation took them by surprise, because they understood that the council still intended to find the causes of the blackout and determine the steps needed to prevent a recurrence. Now those findings will feed into the Energy Department report. The Department of Energy has instructed all parties to preserve relevant data for investigators. The Department of Homeland Security is also part of the government's task force, although "to this point there has been no evidence of any intentional [terrorist] action being involved in this," Abraham said. NERC's press release supporting the U.S.–Canada Task Force investigation is available at [ftp://www.nerc.com/pub/sys/all\\_updl/docs/pressrel/8-20-03-join-task-force.pdf](ftp://www.nerc.com/pub/sys/all_updl/docs/pressrel/8-20-03-join-task-force.pdf)  
Source: [http://www.washingtonpost.com/wp-dyn/articles/A17486-2003Aug\\_19.html](http://www.washingtonpost.com/wp-dyn/articles/A17486-2003Aug_19.html)
2. *August 20, The Arizona Republic* — **Arizona pipeline fails test. A Phoenix-to-Tucson gasoline pipeline that has been shut down since early August because of leaks, ruptured again during tests early Wednesday, August 20. However, the company that owns the pipeline still expects the line to be back in service this weekend.** The company said it is working to replace the faulty section of pipe and will repeat the tests later in the night. The newest leak, in a 4-mile section of the line in northwest Tucson was discovered when the line was filled with water and pressurized to 2,001 pounds per square inch. The federal Office of Pipeline Safety, which approved the test, said the pressure was 139 percent of the line's maximum operating pressure. The company won't be allowed to open the line, which was closed Friday, August 8, until it passes the tests. However, **the federal Environmental Protection Agency temporarily lifted regulations requiring Phoenix to use clean-burning gasoline during the summer.** That will allow fuel from more areas to come into the area.  
Source: <http://www.azcentral.com/news/articles/0820gas-main20-ON.htm>
3. *August 20, Dow Jones Business News* — **Rolling blackouts may be needed in Cleveland. FirstEnergy Corp. warned rolling blackouts may be needed in the greater Cleveland, OH, area Wednesday, August 20, as available power generation is insufficient to cover high weather-related demand.** In a press release, the company called on its customers to take all possible steps to reduce their power consumption. If necessary, FirstEnergy may cut power to industrial and commercial customers that pay lower rates in exchange for agreeing to have their service interrupted when supplies are tight, the utility said. If that isn't sufficient, service could be cut to blocks of customers for two hours at a time, the utility said. FirstEnergy said it has already notified municipalities in greater Cleveland that these procedures may be necessary.  
Source: [http://biz.yahoo.com/djus/030820/1427001020\\_2.html](http://biz.yahoo.com/djus/030820/1427001020_2.html)
4. *August 19, Associated Press* — **Blackout's cost estimated to reach \$6B. The blackout that stranded millions of travelers, halted assembly lines and spoiled tons of food cost an**

**estimated \$4 billion to \$6 billion.** State and local governments, particularly in New York, took the biggest hit from the blackout. New York City comptroller's office estimated that losses topped \$1 billion, including \$800 million in lost gross city product — half of that in the first 24 hours. The figure also includes \$250 million in frozen and perishable foods that had to be dumped, spokesman Michael Egbert said. The blackout cost the city's 22,000 eateries alone between \$75 million to \$100 million in wasted food and lost business, the New York State Restaurant Association calculated. Broadway lost \$1 million worth of tickets for shows canceled after the lights went out Thursday, August 14. Michigan officials remained uncertain of the extent of the effect there, but economists estimated that it will be in the hundreds of millions of dollars. **The airline industry, which lost several days of travel, was in the midst of assessing the damage, and automakers said it still was too soon to estimate blackout related costs but expressed confidence that they will make up most of the lost production.**  
Source: <http://www.nytimes.com/aponline/business/AP-Blackout-Costs.html>

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

## **Chemical Sector**

5. *August 20, TV 11Alive, Atlanta* — **Chemical spill at Gwinnett warehouse. Hazmat crews sealed off a warehouse in Lawrenceville, GA, Wednesday morning due to a potentially toxic chemical spill. Ten people were recovering after being exposed to the hydrofluoric acid which spilled inside of a shipping warehouse located in the 100 block of Boulderbrook Circle in Gwinnett County, authorities say. One person was taken to a local hospital for observation. Authorities said one person actually came in contact with the fluid, which is known to be toxic, as it leaked from a ruptured drum. Both Hazmat and Gwinnett fire rescue teams responded to the situation. They evacuated the warehouse and set up a 400-foot control zone around the warehouse.** There was no official word of any other facilities being affected by the chemical spill or any adjacent roads being sealed off.  
Source: [http://www.11alive.com/news/news\\_article.aspx?storyid=35552](http://www.11alive.com/news/news_article.aspx?storyid=35552)

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

## **Defense Industrial Base Sector**

6. *August 20, Marine Corps Systems Command* — **Marines will soon have a new weapon for riverine operations. The Small Unit Riverine Craft (SURC) was approved for full production in early August. The primary mission of the craft is to provide tactical mobility and a limited weapons platform for the Ground Combat Element of a Marine Air Ground Task Force in littoral and riverine environments.** Later in the program a more heavily armed escort version of the SURC will appear as a replacement to the present Riverine Assault Craft. Together the normal and escort versions will form a team that will increase the flexibility of the ground forces. The craft will also have three weapons mounts that will be interoperable with current and future universal weapon mounts and pintle adapters for tactical vehicles. The SURC will normally be deployed to theatre using strategic air- or sealift and is capable of being flown internally in cargo aircraft as well as externally by a CH-53E.  
Source: <http://www.usmc.mil/marinelink/mcn2000.nsf/main5/1B1BE77B7AF>

7. *August 20, The Birmingham News (AL)* — **Army plans to develop mobile laser for combat. The Army plans to spend about a half-billion dollars over five years to develop a mobile combat laser**, according to an official with that Huntsville, AL-managed program. Development of the tractor-trailer-sized Mobile Tactical High Energy Laser (THEL) prototype begins next year, said Colonel Richard DeFatta, project manager for the Short Range Air Defense. The laser should be ready to begin two years of testing in 2007, he said. **The prototype will be used to develop tactics and procedures for using a mobile laser to shoot down targets such as small rockets, mortar shells and unmanned, remotely piloted airplanes**, DeFatta said. In theory, the prototype could be used in combat, he said. The THEL prototype built by the United States and Israel in the New Mexico desert shot down 33 of 34 targets, including rockets and mortars, in testing in recent years, DeFatta said. Engineers will basically be trying to cut down the size of THEL by about a fourth to fit it on the tractor-trailer-sized vehicle, he said. Like the full-sized THEL, the mobile prototype will be a chemical-fueled laser.

Source: [http://www.al.com/news/birminghamnews/index.ssf?/xml/story.ssf/html\\_standard.xml?/base/news/1061371705244810.xml](http://www.al.com/news/birminghamnews/index.ssf?/xml/story.ssf/html_standard.xml?/base/news/1061371705244810.xml)

8. *August 19, Aerospace Daily* — **Midcourse missile defenses advance on interceptor fronts. The Defense Department's drive to field land- and sea-based midcourse missile defense systems has advanced on several fronts in the past few days, including the successful test of a new interceptor booster for the ground-based program** and a major contract award for the ship-based element. The test of the new interceptor booster for the Ground-based Midcourse Defense (GMD) system appears to have been successful, according to the Missile Defense Agency. **The test, known as Booster Verification-6 (BV-6), was designed to demonstrate the vehicle's silo launch capabilities, verify its design and flight characteristics and confirm the planned performance of its guidance, control and propulsion systems.** Although test results still are being analyzed, the booster appears to have met expectations.

Source: [http://www.aviationnow.com/avnow/news/channel\\_aerospacedaily\\_story.jsp?id=news/mid08193.xml](http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/mid08193.xml)

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

## **Banking and Finance Sector**

9. *August 20, NZX (New Zealand)* — **NZX market closure. The New Zealand Stock Exchange (NZX) market determined Wednesday, August 20, that the electronic messages originating from RMLT, one of the three New Zealand share registries that manage the transfer of shares between brokers accounts and clients accounts, were faulty.** The faults were due to a RMLT software upgrade. NZX management accordingly decided to halt trading in the market. **NZX kept the market closed** until it confirmed conclusively that (i) all shareholder balances within the RMLT registry are correct and all client positions accurate; and that (ii) the message uplift had been restored to NZX's satisfaction. The messaging failure meant that NZX was unable to confirm that transfers of shares were being properly recorded. The real time inability to confirm trades against holdings compromised the integrity of the

market. **NZX has a zero risk tolerance policy and determined the appropriate action was market suspension until market integrity had been restored. NZX was satisfied that the market integrity issues had been resolved later in the day, and normal trading commenced at approximately 4:30 p.m. NZDT.**

Source: [http://www.nzx.com/news/press/release\\_20Aug03\\_3](http://www.nzx.com/news/press/release_20Aug03_3)

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

## **Transportation Sector**

**10. *August 20, Reuters* — U.S. proposes truckers have Hazmat safety permits. The government proposed on Tuesday to require federal safety permits for North American truckers hauling radioactive and toxic material and certain explosives on U.S. roads. "Hazmat cargo represents a large segment of the freight transported daily across America and the (Transportation Department) is committed to ensuring its integrity and security," Transportation Secretary Norman Mineta said in a statement. The September 11, 2001, hijacked airliner attacks prompted new concern about the movement of hazardous materials in the United States, prompting federal government action to close safety and security loopholes. The proposal would require trucking companies from the United States, Mexico and Canada carrying hazardous materials in the United States to register with the government and meet new safety and security standards. Some hazard material cargo would have to be inspected by the government before being hauled. New government safety permits would cover radioactive materials and more than 55 pounds of explosives, including dynamite and nitroglycerin, special fireworks, flash powders and some propellants. Also covered would be liquefied natural gas and toxic substances that are considered dangerous if inhaled.**

Source: [http://publicbroadcasting.net/wnyc/news.newsmain?action=article&ARTICLE\\_ID=535721](http://publicbroadcasting.net/wnyc/news.newsmain?action=article&ARTICLE_ID=535721)

**11. *August 20, PRNewswire* — Computer virus strikes CSX transportation computers. CSX Transportation's (CSXT) information technology systems experienced significant slowdowns early Wednesday after a computer virus infected the network. The cause was believed to be a worm virus similar to those that have infected the systems of other major companies and agencies in recent days. The infection resulted in a slowdown of major applications, including dispatching and signal systems. As a result, passenger and freight train traffic was halted immediately, including the morning commuter train service in the metropolitan Washington, DC area. Contrary to initial reports, the signal system for train operations was not the source of the problem. **Rather, the virus disrupted the CSXT telecommunications network upon which certain systems rely, including signal, dispatching and other operating systems.** CSXT's technology and operating teams immediately began aggressive and comprehensive efforts to restore the computer system and service to rail passengers and freight customers. Many key systems had been restored as of midday, allowing for resumption of substantial operations as the company works toward full system capability. CSX Corporation, based in Jacksonville, FL, owns the largest rail network in the eastern United States.**

Source: [http://biz.yahoo.com/prnews/030820/flw012\\_1.html](http://biz.yahoo.com/prnews/030820/flw012_1.html)

12. *August 20, Chicago Sun Times* — **Planes in last two months fullest since 1970. U.S. airliners in the last two months were the most crowded in at least 30 years, mainly because the carriers have parked more than 600 aircraft amid slow demand and efforts to reduce costs. Planes of the biggest U.S. carriers, including American Airlines and United Airlines, on average were 82 percent full in July, the highest since 1970, when the Air Transport Association began recording the statistic.** In June, aircraft were 80 percent full on average. U.S. airlines have grounded planes since the September 11, 2001, attacks, and seat capacity for the top 10 U.S. carriers in July fell 6 percent from last year and 10 percent from July 2000, before the terrorist attacks curtailed air travel. The industry has posted more than \$20 billion in losses because less passenger demand has meant lower prices and revenue. Of the 10 largest U.S. carriers, Houston-based Continental Airlines had the highest loads, with planes 84.5 percent full on average, followed by ATA, an Indianapolis-based low-fare carrier operating mainly from Chicago, which had loads of 84.3 percent.

Source: <http://www.suntimes.com/output/business/cst-fin-airlines20.html>

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

## Postal and Shipping Sector

Nothing to report.

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

## Agriculture Sector

13. *August 20, Bloomberg* — **China, Brazil, India seek limit to farm aid. China, Brazil, and India, which together account for more than \$50 billion in agricultural exports a year, called on the United States, European Union, and other industrialized nations to slash their farm subsidies. In a joint proposal to negotiators at the World Trade Organization, the three nations demanded a cap to spending on environmental or rural development programs and cuts to other domestic aid payments. They also called for the phasing out of subsidies that finance exports of all commodities, such as sugar, cotton, and grains.** The paper follows an agreement in principle by the U.S. and EU last week to reduce farm aid. Today's paper is a "direct challenge" to the EU-U.S. plan, "which would have left billions of dollars in export subsidies intact," aid agency Oxfam said in an e-mail. While the U.S. and EU called for hefty cuts in duties, they stopped short of agreeing to eliminate export subsidies completely, one of many agricultural exporters' main priorities. **Industrialized nations spent \$311 billion to help their farmers in 2001, according to the Organization for Economic Cooperation and Development.**

Source: <http://quote.bloomberg.com/apps/news?pid=10000080&sid=ahdma32Rxibk&refer=asia>

14. *August 20, Seattle Post-Intelligencer* — **Building a better egg through science.** Max Hincke, a University of Ottawa scientist, is part of an international research group called EggDefense looking for genetic clues as to how to make eggshells stronger. **The scientists want to reduce tiny cracks that can allow bacteria such as salmonella to gain a foothold.** Chickens make eggshells in a process that involves minerals and proteins. **Hincke has isolated and sequenced**

**the genes for 10 proteins that influence formation of the eggshell, and says two or three dozen more may be involved.** He and his colleagues have identified two genes for proteins that form sort of a mesh throughout the eggshell. These so-called "matrix proteins" make up only a small portion of the eggshell. But they are important because they influence how the hard mineral that makes up 95 percent of the shell, calcium carbonate, crystallizes as the shell is being built.

Source: [http://seattlepi.nwsourc.com/food/135693\\_tf120.html](http://seattlepi.nwsourc.com/food/135693_tf120.html)

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

## Food Sector

15. *August 20, Associated Press* — **Michigan meat company recalls beef products for possible contamination. A Detroit meat processor has issued a voluntary recall of about 3,600 pounds of fresh beef products that the federal government said were processed under unsanitary conditions.** The U.S. Department of Agriculture's Food Safety and Inspection Service said the products were produced by Mark's Quality Meats, Inc. on August 15 and 16 and distributed to restaurants in the Detroit area. Agriculture Department and company officials were concerned about the water that was used to clean the meat processing equipment, company spokesman Fred Marx said Wednesday. **Michigan residents and businesses had been asked to boil their water before using it because last week's blackout may have caused some bacterial contamination. "The water had not been given the all clear when it was used to clean the machine," Marx said.** The company was not aware of any illnesses that the meat had caused.

Source: [http://www.mlive.com/newsflash/michigan/index.ssf?/newsflash/get\\_story.ssf?/cgi-free/getstory\\_ssf.cgi?g8020\\_BC\\_MI--Blackout-MeatReca&&news&newsflash-michigan](http://www.mlive.com/newsflash/michigan/index.ssf?/newsflash/get_story.ssf?/cgi-free/getstory_ssf.cgi?g8020_BC_MI--Blackout-MeatReca&&news&newsflash-michigan)

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

## Water Sector

16. *August 20, Associated Press* — **Scientist hopes bacteria could cleanse toxic water supplies. An Australian scientist has discovered a toxin eating bacteria that could clean up arsenic-tainted water drunk by millions of Bangladeshis, a report said this week.** "We hope the bacteria will one day be used in bioremediation, where bacteria that eat arsenic will be used to clean up the contaminated water," said microbiologist Joanne Santini. She found the unusual bacteria in gold mines in Australia's Northern Territory and Victoria state. The find could help eliminate arsenic in water drunk by thousands of villagers in Bangladesh, said Santini. **She said the new bacteria converted arsenic into a nontoxic form called arsenite that could easily be filtered out of water. More studies were needed before the bacteria could be used.** The United Nations warned in a 2001 report that nearly 57 million people in Bangladesh could get cancer from drinking arsenic-tainted well water. More than 4 million wells were sunk across Bangladesh in a U.N. campaign since 1970. At least half those wells are contaminated with arsenic, according to Bangladesh government estimates. **Arsenic occurs naturally in rocks and is commonly released by mining activity. Santini said old**

contaminated mines could also benefit from the discovery.

Source: [http://www.enn.com/news/2003-08-20/s\\_7624.asp](http://www.enn.com/news/2003-08-20/s_7624.asp)

17. *August 20, Florida Sun Sentinel* — **Unsanitized water pipes. For the past five or six years, Fort Lauderdale, FL, water pipes stored in an open field were hooked up to homes or businesses without being properly disinfected, a State Attorney's Office investigation found.** The investigation, closed Friday by Assistant State Attorney John Countryman, backed up allegations made by a former city employee that the city didn't properly disinfect pipes shorter than 50 feet before connecting buildings to the water supply or after making small repairs. Initially, city staff had denied any problem. But the scrutiny brought on by Countryman's subpoenas, prompted them to acquiesce. **After consultations with other cities and with health officials, Fort Lauderdale has begun sanitizing the pipes it formerly flushed only with tap water.** The pipes are of any dimension and include service lines that connect homes or businesses to water mains as well as large water mains that serve thousands. **City officials contend the drinking water was safe all along, and that regular, required testing proves that.** Countryman found that the pipes were stored "in an open field near a wooded area where they might easily collect debris and dirt" and confirmed they were flushed with tap water.

Source: <http://www.sun-sentinel.com/news/local/southflorida/sfl-cwater20aug20.1.4847672.story?coll=sfla-home-headlines>

[[Return to top](#)]

## **Public Health Sector**

18. *August 20, New Scientist* — **SARS virus may be back in Canada. An outbreak of pneumonia, which tests so far indicate may be caused by the Severe Acute Respiratory Syndrome (SARS) virus, appears to be spreading in British Columbia, Canada. The virus has already infected over 150 people and killed six at a nursing home near Vancouver, and now appears to have infected a second nursing home nearby. Nine residents at another, unidentified nursing home in the region are reported to have the same symptoms.** Researchers have announced that several genetic sequences from the virus are identical to the virus that causes SARS. But, confusingly, the symptoms shown in the new outbreak have been much milder. Efforts to culture the mystery virus have so far been unsuccessful. But Frank Plummer, director of the Winnipeg lab, told reporters that some 800 base pairs in four of its gene regions had sequences identical to the SARS virus in seven out of eight samples. In the eighth, the sequence differed by only one base pair.

Source: <http://www.newscientist.com/news/news.jsp?id=ns99994078>

19. *August 20, AScribe NewsWire* — **Prion infectivity. In experiments with yeast prions, Howard Hughes Medical Institute researchers have shown how point mutations in prions, which do not compromise their infectivity, can nevertheless cause prions to alter the specificity of the yeast strain that they infect. According to the researchers, their findings point the way to studies that could begin to clarify the factors that determine whether a prion specific to cattle that causes bovine spongiform encephalopathy (BSE) might become infectious to humans.** The studies also suggest a new approach for treating disorders such as Alzheimer's disease that involve aberrant protein folding, said the researchers. It might

be possible to develop drugs that would influence toxic proteins that aggregate into brain-clogging plaque to fold into less toxic versions, they said. Unlike bacteria and viruses, prions consist only of aberrant proteins that misfold themselves into forms that, in turn, induce their normal counterparts to misfold. In mammalian prion infections, these abnormal, insoluble proteins trigger protein clumping that can kill brain cells. In humans, clumping causes fatal brain-destroying human diseases such as Creutzfeldt–Jakob disease and kuru, and in animals it causes BSE and scrapie.

Source: [http://www.ascribe.org/cgi-bin/spew4th.pl?ascribeid=20030820\\_092513&time=10%2002%20PDT&year=2003&public=1](http://www.ascribe.org/cgi-bin/spew4th.pl?ascribeid=20030820_092513&time=10%2002%20PDT&year=2003&public=1)

**20. August 20, Health Day News — Radioactive particles treat disease. In a research first, scientists successfully treated an infectious disease by piggy-backing radioactive particles onto antibodies, which zero in on disease-causing microbes without causing harm to healthy cells. This procedure known as radioimmunotherapy may offer a new way to fight diseases caused by a number of bacteria, fungi, protozoa, and other organisms.** In their study, the researchers affixed isotopes to antibodies and demonstrated that the microbe killing ability of ionizing radiation can be harnessed for clinical use. The researchers targeted their radioimmunotherapy against a major fungal pathogen called *Cryptococcus neoformans*. Mice were infected with the fungus then the researchers injected them with varying concentrations of one or another of antibody preparations containing two different radioisotopes. Some other mice were infected with the fungus but not treated. The mice treated with either of the radiolabeled antibodies lived much longer than untreated mice and suffered no apparent toxicity from the treatment. The study also found that, 48 hours after treatment, the mice treated with radioimmunotherapy had greatly reduced levels of fungi in their lungs and brains compared with untreated mice.

Source: <http://www.healthscout.com/template.asp?page=newsdetail&ap=1 &id=514705>

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

## **Government Sector**

Nothing to report.

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

## **Emergency Services Sector**

**21. August 20, Federal Computer Week — Coast Guard tests digital photo transmission.** Coast Guard first responders may soon be able to transmit photos directly from incident scenes to command centers. **A testing program has begun this month in San Francisco to determine the effectiveness of combining wearable computers with digital photography in an On-Scene Photo Documentation Kit.** Officials for the Coast Guard expect to use real-time data from the kit to plan quicker responses to emergencies. Transmitted data also can be shared more efficiently with partners such as state and local law enforcement agencies. The kit sends the photos to a secure command center Web site, also developed by Anteon, via a wireless commercial network. **An integrated global positioning system tags each photo with the latitude and longitude of the incident's location.**

Source: <http://www.fcw.com/fcw/articles/2003/0818/web-wear-08-19-03.asp>

22. *August 20, Rand Report* — **Summary of report: Protecting Emergency Responders. The report "Protecting Emergency Responders Volume 2: Community Views of Health and Safety Risks and Personal Protection Needs" is the second in a series of RAND studies on protecting emergency responders.** The first report outlined the findings of a special conference of emergency workers who responded to the bombing of the Murrah Federal Building in Oklahoma City, the terrorist attacks of September 11, 2001, and the anthrax incidents that occurred during autumn of 2001. Police, firefighters, medical technicians and other responders to emergencies around the United States believe they have inadequate protection against some of the dangers they face, particularly terrorist attacks, according to a RAND study issued today. **"The majority of emergency responders feel vastly underprepared and underprotected for the consequences of chemical, biological, or radiological terrorist attacks,"** says the study prepared by RAND's Science and Technology Policy Institute. The emergency workers, who respond to fires, vehicle collisions, medical emergencies, crimes, natural disasters, terrorist attacks and every other conceivable emergency, want better protective clothing and equipment, more compatible communications systems, and expanded training and information on safety practices and equipment, RAND researchers found.
- Source: <http://www.rand.org/publications/MR/MR1646/>

23. *August 20, The Christian Science Monitor* — **Small fire stations losing volunteers. Many small towns face a dearth of emergency responders as cities forbid their crews from serving other towns in their spare time.** The Rocky Hill, CT, fire chief says career firefighters in nearby Hartford, CT, are forbidden to volunteer in hometown fire stations. In a new contract with its career firefighters, the city forbids them to volunteer at their hometown fire stations. The Hartford chief cites health and safety concerns. Chief Kochanek, who will lose two of his most qualified men, cites indignation. With Kochanek in the thick of it, the town of Rocky Hill and several of its suburban neighbors have launched a fight to try to get the provision removed from the Hartford contract. **They contend it violates the firefighters' First Amendment rights, and just as important, the spirit of volunteerism on which so much of small-town life is dependent. Their ire is shared by others in almost a dozen other states from Virginia to Oregon, where big-city departments are making it harder for career firefighters to work the hoses on their hometown ladder trucks. Indeed, it's turned into a morality tale of sorts about the challenges of modern-day civic life.** For small towns dependent on a steadily shrinking base of volunteers, it's become a threat to the very existence of their fire departments.
- Source: <http://www.csmonitor.com/2003/0820/p02s01-usec.html>

24. *August 19, Associated Press* — **Ham radio operators step into the breach when technology failed. When technology failed on a massive scale last week, some old-fashioned broadcasting stepped into the breach as ham radio operators took to the airwaves to reach emergency workers.** For millions of people in the Northeast and Midwest last week's massive blackout took access to e-mail and the Internet with it. Landline and cellular telephones were jammed by a crush of calls. **But the ham radio, which came into being in the World War I era, connected firefighters and police departments, Red Cross workers and other emergency personnel during the most extensive blackout in the Northeast since**

**1977. Ham operators are not dependent on a server or cell tower, and with battery backup can operate when grids fail. "When everything else fails, the ham radio is still there," said Allen Pitts, a ham operator in New Britain. "You can't knock out that system."** The radios are operated by a network of volunteers organized by the Newington-based American Radio Relay League. Ham radio's importance won renewed recognition after the terrorist attacks of September 11, 2001. The organization won a federal Homeland Security grant of nearly \$182,000 to train amateur radio operators in emergency operations to help during terrorist attacks.

Source: <http://www.stamfordadvocate.com/news/local/state/hc-19021723.apds.m0797.bc-ct--blacaug19.0.5869394.story?coll=hc-headlines-local-wire>

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

## **Information and Telecommunications Sector**

**25. August 20, Microsoft — Microsoft Security Bulletin MS03-032: Cumulative Patch for Internet Explorer. There is a vulnerability involving the cross-domain security model of Internet Explorer which keeps windows of different domains from sharing information.** An attacker could load malicious script code onto a user's system in the security context of the My Computer zone and run an executable file that was already present on the local system or view files on the computer. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately. **The patch also prevents the BR549.DLL ActiveX control from running or from being reintroduced onto users' systems by setting the Kill Bit on the control; changes the way Internet Explorer renders HTML files** which addresses a flaw in the way Internet Explorer renders Web pages that could cause the browser or Outlook Express to fail; and **contains a modification to the fix for the Object Type vulnerability** corrected in Microsoft Security Bulletin MS03-020 which corrects the behavior of the fix to prevent the attack on specific languages.

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-032.asp>

**26. August 20, Microsoft — Microsoft Security Bulletin MS03-033: Unchecked Buffer in MDAC Function Could Enable System Compromise.** When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. **Due to a flaw in a specific Microsoft Data Access Components (MDAC) component, an attacker could respond to this request with a specially crafted packet that could cause a buffer overflow.** An attacker could then gain the same level of privileges over the system as the application that initiated the broadcast request. This could include creating, modifying, or deleting data on the system, reconfiguring the system, reformatting the hard disk, or running programs of the attacker's choice. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-033.asp>

**27. August 20, Dow Jones Newswire — Sobig virus spread is fastest ever. The "Sobig.F" computer virus that began attacking e-mail systems globally Tuesday, August 19, has**

been declared the fastest-spreading e-mail virus of all time. E-mail filtering company MessageLabs Inc. said it intercepted more than one million copies of Sobig.F Tuesday, the most ever in a single day. **The interception rate was one in every 17 e-mail messages the firm scanned. Sobig.F continued to spread aggressively Wednesday.** Sobig.F, which is the sixth and latest strain of a virus that first emerged in January, spreads through Windows personal computers via e-mail and network file-share systems. Besides clogging e-mail systems full of messages with subjects like "Re: Details" and "Re: Wicked screensaver," **the virus also deposits a Trojan horse, or hacker back door, that can be used to turn victims' PCs into spam machines.** The worm is programmed to stop spreading on September 10.

Source: [http://news.yahoo.com/news?tmpl=story2&cid=808&u=/dowjones/20030820/bs\\_dowjones/200308201654001134&printer=1](http://news.yahoo.com/news?tmpl=story2&cid=808&u=/dowjones/20030820/bs_dowjones/200308201654001134&printer=1)

28. *August 18, ZDNet* — **In MSBlast's wake, a DirectX threat.** Microsoft seems to have survived the MSBlast worm attack, but now **the company is urging Windows users to patch their systems against a different, and potentially more dangerous, vulnerability in its software. On July 23, Microsoft posted a security bulletin on its Web site that describes a "critical" vulnerability in DirectX.** According to the company, unprotected systems could be at the mercy of an attacker by simply playing a midi file or visiting a malicious Web page. A specially designed MIDI file could cause a buffer overflow error and either pass control of the system to an attacker, cause damage to the system or use the system to set off another MSBlast-type attack. The DirectX patch is available from Microsoft's Web site:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-030.asp>.

Source: [http://zdnet.com.com/2100-1105\\_2-5065096.html](http://zdnet.com.com/2100-1105_2-5065096.html)

### Internet Alert Dashboard

Current Alert Levels	
 <p>AlertCon: 2 out of 4 <a href="https://gtoc.iss.net">https://gtoc.iss.net</a></p>	 <p>Security Focus ThreatCon: 3 out of 4 <a href="http://analyzer.securityfocus.com/">http://analyzer.securityfocus.com/</a></p>
Current Virus and Port Attacks	
<b>Virus:</b>	#1 Virus in the United States: <b>WORM_SOBIG.F</b> Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
<b>Top 10 Target Ports</b>	135 (epmap), 445 (microsoft-ds), 137 (netbios-ns), 80 (www), 1434 (ms-sql-m), 1433 (ms-sql-s), 443 (https), 17300 (Kuang2TheVirus), 139 (netbios-ssn), 27374 (SubSeven) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center

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

## General Sector

**29. *August 20, Associated Press* — Navy chopper loses radioactive part over North Carolina.**

**North Carolina state officials say a Navy helicopter blade inspection system containing a small amount of radioactive Strontium 90 fell off a Navy chopper in Onslow County, NC, on Friday, August 8.** The part is unlikely to pose a threat to anyone who might find it because Strontium does not emit radiation over long distances. The radioactive material is the size of a golf tee welded within metal foil and inside a silver stainless steel case. The part may also be covered in a plastic housing. Fliers are being distributed to area farm workers and other residents urging anyone who finds the part to note the exact location and call the state Division of Emergency Management.

Source: <http://www.wral.com/news/2419549/detail.html>

**30. *August 20, Associated Press* — Severe storms flood Las Vegas, trapping motorists and prompting a state of emergency. Flood waters receded Wednesday and residents began the messy job of cleaning up after intense storms swamped some neighborhoods, knocking out power to thousands and leaving motorists stranded atop their cars. The deluge Tuesday caught many by surprise, as it dumped three inches of rain in 90 minutes, severely flooding the city's northwest section. Casinos along the Las Vegas Strip saw only light rainfall.** "There was so much water, we couldn't see the sidewalks," said Ann Friary, owner of Northshore Learning Tree, a day care center. At least two motorists had to be rescued from the tops of their cars by a helicopter. Four firefighters were rescued from a fire engine that became trapped by raging floodwaters. **At the height of the storms, some 3,000 customers briefly lost power, Nevada Power said, although electricity was restored to all but about 300 within a few hours. Mayor Oscar Goodman declared a local state of emergency and urged people to stay at home and keep off the roads.** More thunderstorms were in the forecast for Wednesday, the National Weather Service, said but the most severe storms were expected to remain just outside the area.

Source: <http://www.fema.gov/press/ap/ap082003.shtm>

[[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](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at 703-883-6631

Subscription and Distribution Information Send mail to [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at 703-883-6631 for more information.

**Contact DHS/IAIP**

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov) or call 202-323-3204.

**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.