



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 16 July 2004

Current Nationwide
Threat Level is



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

www.whitehouse.gov/homeland

Daily Overview

- IDG News Services reports that an online shop that was selling the source code for two computer programs from Fortune 100 software companies has abruptly suspended its operations. (See item [7](#))
- The Seattle Times reports that the Transportation Security Administration (TSA) acknowledged Wednesday, July 14, that independent government agents are investigating security lapses at William P. Hobby Airport in Houston, TX. (See item [10](#))
- Security officials are deploying more than a half–dozen mobile command vehicles around Greater Boston during the Democratic National Convention to ensure that communication among law enforcement and rescue agencies continues in the event of a terrorist attack, according to the Boston Globe. (See item [27](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [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 Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [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. *July 15, Associated Press* — OPEC to increase oil production. With the price of oil stuck above \$40 a barrel, the Organization of Petroleum Exporting Countries (OPEC) agreed Thursday, July 15, to raise its daily production target by 500,000 barrels, or two percent, in an effort to keep crude prices from lurching even higher. Although oil–exporting countries are happy to maximize profits, OPEC and its de facto leader Saudi Arabia worry that

global economic growth and the long-term demand for crude could suffer if prices spike to punishing heights. However, few analysts expect the increase in OPEC's target to do much to reduce prices from current levels. Most of the group's members are already pumping all they can to satisfy strong demand, and oil markets had already factored the increase into prices. OPEC pumps more than a third of the world's oil. The increase will take effect August 1.
Source: http://www.washingtonpost.com/wp-dyn/articles/A51890-2004Jul_15.html

2. *July 15, Government Accountability Office* — **GAO-04-982T: Energy Markets: Mergers and Other Factors that Affect the U.S. Refining Industry (Testimony)**. Gasoline is subject to dramatic price swings. A multitude of factors affect U.S. gasoline markets, including world crude oil costs and limited refining capacity. Since the 1990s, another factor affecting U.S. gasoline markets has been a wave of mergers in the petroleum industry. For example, in 1999, Exxon, the largest U.S. oil company, merged with Mobil, the second largest. This testimony is based primarily on Energy Markets: Effects of Mergers and Market Concentration in the U.S. Petroleum Industry (GAO-04-96, May 17, 2004). **This report examined mergers in the industry from the 1990s through 2000, the changes in market concentration (the distribution of market shares among competing firms) and other factors affecting competition in the industry**, how U.S. gasoline marketing has changed since the 1990s, and how mergers and market concentration in the industry have affected U.S. gasoline prices at the wholesale level.
Source: <http://www.gao.gov/new.items/d04982t.pdf>

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

Chemical Industry and Hazardous Materials Sector

3. *July 15, The Courier News (IL)* — **Flaming truck forces closing of interstate. A stretch of Interstate 88 at Illinois 47 was closed for several hours Wednesday, July 14, when a truck carrying a mixed load of flammable powders and liquids caught fire and exploded several times.** Sgt. Jim Jenker of the Illinois State Police said a trooper spotted flames coming from the westbound vehicle and signaled the driver to pull over and stop at about 12:30 a.m. **Officials said the 53-foot semitrailer, owned by Nationwide Express, was carrying chloride, phosphate and ether in both liquid and solid form in containers such as metal drums, plastic totes and bags.** The truck was bound for St. Paul, MN, from Chicago, IL. Both sides of the interstate were shut down to traffic for nearly seven hours. For most of the day, the right westbound lane remained closed to motorists as a certified hazardous materials company cleaned up the scene.
Source: http://www.suburbanchicagonews.com/couriernews/city/e15i88cr_ash.htm

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

Defense Industrial Base Sector

4. *July 15, NetDefense* — **JFCOM seeks industry to help. U.S. Joint Forces Command (JFCOM) is asking industry and academia for help in developing and testing technology that will improve the interoperability of unmanned aerial vehicles (UAV) and related**

intelligence, surveillance, and reconnaissance capabilities. JFCOM plans to hold a series of experiments in the next fiscal year to test interoperability solutions, possibly in the fall of this year, as well as the early spring and summer of 2005. JFCOM is looking to industry for a range of capabilities, including advanced radar, signal intelligence, and other intelligence sources, said Frank Roberts, head of UAV initiatives in the Intelligence, Surveillance, and Reconnaissance Integration Division in J2. Information from sensors, whether from UAVs, from the ground, or from a soldier, "needs to get into the network" so that the data can be accessed by a warfighter, said Roberts.

Source: http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/uav07154.xml

[[Return to top](#)]

Banking and Finance Sector

5. *July 15, The Scotsman (Scotland)* — **Police raid smashes counterfeit euro ring.** Colombian police and Interpol have broken what they believe was Latin America's first major ring to print fake euros. A raid in Bogotá uncovered printing presses, 54,400 in fake notes and \$104,700 of counterfeit U.S. dollars. Two people were arrested. Pamphlets related to the country's largest rebel group, the Revolutionary Armed Forces of Colombia, were found during the raid, said a detective with the international police agency Interpol. **Colombia is the world's most prolific counterfeiter of American dollars, with fake notes with a face value of more than \$150 million discovered in the past four years. Authorities said the fake euros discovered on Sunday, July 11, were of high quality.**

Source: http://thescotsman.scotsman.com/international.cfm?id=8077620_04

6. *July 15, Washington Post* — **Bush signs identity theft bill.** President Bush signed a tough new identity theft bill into law on Thursday, July 15 — legislation passed by Congress in response to evidence that the problem is growing rapidly as more Americans use the Internet to shop and manage their personal finances. **The Identity Theft Penalty Enhancement Act adds two years to prison sentences for criminals convicted of using stolen credit card numbers and other personal data to commit crimes. Violators who use that data to commit "terrorist offenses" would get five extra years. The law will make it more likely that thieves are prosecuted,** said Betsy Broder, assistant director for the Federal Trade Commission's Division of Planning and Information. "A prosecutor is less likely to bring a case if they're not going to get any serious jail time when the get a conviction," Broder said. Identity theft topped the list of consumer fraud complaints to the Federal Trade Commission in 2003, accounting for more than half of all the complaints tracked by the agency. The law also orders the U.S. Sentencing Commission to consider increasing the penalties for employees who steal sensitive data from their own companies.

Source: http://www.washingtonpost.com/wp-dyn/articles/A51595-2004Jul_15.html

7. *July 15, IDG News Service* — **Hacker source code shop closes its doors. An online shop that was selling the source code for two computer programs from Fortune 100 software companies has abruptly suspended its operations, citing a "redesign" of its "business model." The Source Code Club opened its doors on Monday, July 12, using an e-mail posting to an online discussion group to advertise the availability of source code and**

design documents for two products: the Dragon intrusion detection system (IDS) software from Enterasys Networks Inc. and peer-to-peer (P-to-P) server and client software from Napster LLC. By Thursday, July 15, the group's Web page displayed a message saying the club had ceased operations due to "fears our customers faced." The group used a Web page with an address in the Ukraine to advertise its wares, saying it was selling "corporate intel(ligence)" to its customers, along with other, unnamed, services, according to a message posted to the Full-Disclosure mailing list. On Thursday, the club's Web site was renamed the "former SCC page," with the group saying it plans to re-emerge, but that it needed to change its business model to ease customers' fears. Enterasys is working with the Federal Bureau of Investigation to investigate the club's claims, according to Kevin Flanagan, an Enterasys spokesperson. Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,94552,00.html>

8. *July 07, Security Pipeline* — **Phishing attacks linked to organized crime. Federal and state law enforcement officials have linked organized crime to phishing attacks that are increasing in both volume and sophistication. "There's a lot of activity in the former Soviet bloc, the Eastern bloc, Latvia, and Ukraine,"** says John Curran, supervisory special agent with the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center. While Curran notes that a broad array of criminals appears to be involved in phishing attacks, the FBI is investigating links to organized crime. The U.S. Secret Service has also noted an increase in organized crime involvement in phishing. Dan Maier, a spokesperson for the Anti-Phishing Working Group (APWG), an industry forum, believes that organized crime participation in phishing has been increasing. "Early on it was amateurs," Maier acknowledges, however "there are a number of attacks against Australian banks that point back to Asian gangs. **We can tell by looking at the nature of some of the attacks, the ones that use common elements and Websites, that multiple attacks are linked.**" APWG has been working with the U.S. Secret Service and the FBI, but Maier says it has been difficult to prosecute these crimes because many of the attacks originate from foreign countries. Source: <http://www.securitypipeline.com/showArticle.jhtml?articleId=22104197&pgno=1>

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

Transportation Sector

9. *July 15, Record Herald (PA)* — **Bomb threat brings traffic to a standstill. Interstate 81 was shut down for more than an hour Tuesday, July 14, for a terrorist scare that turned out to be an apparent idle threat. A truck driver near Carlisle, PA, called Pennsylvania State Police to say he had gotten into an argument on his CB radio with a man who sounded like he was of Middle Eastern descent. The driver told police the other man had said he was carrying explosives in his truck.** Based on that information, Maryland State Police stopped the driver of a yellow tractor pulling a white box trailer around 12:20 p.m. south of Halfway, PA, on I-81. Police closed the interstate for about 75 minutes as a precaution, backing up traffic in both directions. The Hagerstown, MD, City Police bomb dog was brought in to search the truck for explosives but found nothing, according to police reports. Members of the Washington County, MD, Special Operations team, dressed in protective clothing, searched for chemicals and biological contaminants, police said. They did not find anything. The driver was interviewed at state police barracks in Hagerstown and released without being charged around 5:00 p.m. The investigation into the circumstances of the incident is continuing, police

said.

Source: http://www.therecordherald.com/articles/2004/07/14/local_news/news03.txt

10. **July 15, *Seattle Times* (WA) — Security at Houston airport being probed. The Transportation Security Administration (TSA) acknowledged Wednesday, July 14, that independent government agents are investigating security lapses at William P. Hobby Airport in Houston, TX.** In a *Seattle Times* series on security problems at airports across the country published recently, screeners and supervisors from Houston complained that managers had directed that luggage go unscreened for weapons or explosives before being put on flights. The screeners complained to a Texas congressional delegation after one such lapse in March. During that incident screeners say they ignored an order and examined every bag they touched. However, two managers stepped in and threw bags onto the outgoing conveyor belt themselves. One screener counted more than 80 bags that went unscreened, according to interviews and the screeners' letter to Congress. TSA is awaiting the results of the investigation and doesn't know when it will be completed, said spokesperson Jennifer Marty.
Source: <http://archives.seattletimes.nwsource.com/cgi-bin/taxis.cgi/web/vortex/display?c=1&slug=tsa15&date=20040715&query=philli ps>
11. **July 14, *Government Executive* — U.S. Coast Guard reauthorization bill approved by conferees. House and Senate conferees Wednesday, July 14, quickly approved a \$7.9 billion reauthorization measure for the U.S. Coast Guard in fiscal year 2005, preparing the bill for a final House floor vote next week.** The bill (H.R. 2443) would provide the Coast Guard with \$5.4 billion for operations and expenses; \$1.5 billion for acquisition, construction and improvements; \$24.2 million for research and development; \$1.08 billion for retirement pay; \$1.86 million for bridge improvements and \$17 million to comply with environmental requirements.
Source: http://www.govexec.com/story_page.cfm?articleid=28987&dcn=to_daysnews
12. **July 14, *United Press International* — New rail security for Connecticut. Department of Homeland Security (DHS) Undersecretary Asa Hutchinson said the rail-security program started in New Carrollton, MD, after the terrorist attacks on Madrid's rail system has been successful and will be expanded on passenger trains in Connecticut.** Hutchinson said Tuesday, July 13, that the first and second phases of the pilot program, which tested explosives-detection equipment at the New Carrollton Amtrak station and Washington, DC's Union Station, were important steps toward improving U.S. railroad security. The new test will be the last of a series implemented to evaluate methods for screening passengers in a specific area or on a specific train. The explosives-detection pilot program in New Carrollton used a private vendor's system, which can determine the presence of explosives from a small air sample. The system has been tested in airports, but rail stations are considered to be a more difficult environment in which to use explosives-detection technology. The final phase of the test is likely to employ another variation of explosives-detection technology in a format that can easily fit into a moving train car.
Source: <http://washingtontimes.com/business/20040714-110111-1177r.htm>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

13. *July 15, Ellsworth American (ME)* — **Blueberry crop outlook grim. David Yarborough, the University of Maine's extension office blueberry specialist, estimates that Maine's blueberry crop yields will be down by an overall 30 percent.** He said the area didn't get the amount of snow cover it generally receives and much of the area experienced a very wet spring. Yarborough said the snow cover acts as an insulator against the cold protecting the plant's new growth where the berries will set. "We're seeing a lot of bushes with buds appearing near the bottom of the plants only," he said. **He also said that many areas are experiencing fungus disease blight due to wet conditions.**

Source: http://www.ellsworthamerican.com/archive/2004/07-15-04/ea_news4_07-15-04.html

14. *July 15, PR Newswire* — **Alert system for Georgia. Two telecommunications companies have been on a one-year contract to deliver a Web-based emergency alert system for use by key agricultural agencies in Georgia in the event of a crisis, such as an animal disease outbreak or contamination of the state's food supply.** The system, called CHAIN-EMN, is a secure, reliable, web-based, two-way communication and alert reporting system that can rapidly disseminate information via a range of devices that include telephones, PCs, PDAs, cell phones and other means. Participants can access or receive messages regardless of the device or network carrier they are using. The alert notification project is being directed by the Georgia Department of Agriculture for the Agriculture Information Sharing and Analysis Center (AGISAC), a network of federal and state agencies, private sector companies and academic institutions, as well as agriculture associations based in Georgia. CHAIN-EMN will allow participants to simultaneously send alerts to key agencies, organizations, specific groups or individuals describing potential threats, recommending next steps and providing updates. Recipients receive the information rapidly over virtually any communications device and can respond to and collaborate with the sender -- potentially preventing or mitigating the impact of a threat.

Source: <http://www.tmcnet.com/usubmit/2004/Jul/1056964.htm>

15. *July 14, Minda News (Philippines)* — **Animal disease spreads in Philippines. The provincial veterinarian's office of North Cotabato has urged Governor Emmanuel F. Piñol to put the whole province under a state of calamity due to the spread of an infectious blood disease that affects farm animals. The disease, called surra, has reportedly already spread 12 towns in the province.** Based on reports gathered by the veterinarian's office, 135 farm animals have died in these areas since last year. Enrico Garzon, the provincial veterinarian, told MindaNews that last month, 16 carabaos and 19 horses died suddenly in Makilala town apparently due to surra disease. The provincial government, the office of the provincial veterinarian and the college of medicine of the University of Southern Mindanao in Kabacan, North Cotabato have conducted random blood sampling in the 12 affected towns where surra disease was observed. The team collected and tested 1,430 blood samples of which 32 percent tested positive.

Source: <http://www.mindanews.com/2004/07/14nws-surra.html>

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

Food Sector

16. *July 15, Associated Press* — **Mandatory testing would still miss cattle. Mandatory testing of cattle for mad cow disease would not improve on the current voluntary system because the government still could never be sure producers were complying, said Ron DeHaven, administrator of the Animal and Plant Health Inspection Service Wednesday, July 14.** He said that relying on cooperation from farmers, slaughterhouse operators, and renderers is working well in coming up with brain tissue samples to be checked for the fatal brain-wasting disease. Mandatory testing also would mean time-consuming rule-making, DeHaven said. U.S. Department of Agriculture (USDA) officials said the surveillance system is only designed to assess the possible extent of mad cow in the U.S. and is not aimed at protecting the food supply. Food is protected by other programs, including regulations that bar the use of tissue such as brains and spinal cords from the human food supply. Those animal parts may harbor the misshapen proteins called prions that can transmit Mad cow.

Source: http://www.yankton.net/stories/071504/new_20040715013.shtml

17. *July 14, Associated Press* — **Salmonella outbreak sickens 34 in Pennsylvania. Nearly three dozen cases of salmonella poisoning throughout western Pennsylvania have been traced to a convenience store chain, health officials said.** The 34 cases have been traced to Sheetz stores, said Richard McGarvey, spokesperson for the state Department of Health. All have been linked to a type of bacteria most commonly found on fresh produce; state health officials have not pinpointed the source. Those who have gotten ill had purchased food at different Sheetz stores, which pointed to an outside supplier, McGarvey said. The cases were reported by doctors or hospitals mainly in western Pennsylvania. The figure was expected to rise, McGarvey said.

Source: http://www.mlive.com/newsflash/national/index.ssf?newsflash/get_story.ssf?cgi-free/getstory_ssf.cgi?a0827_BC_SalmonellaOutbreak&&news&newsflash-national

18. *July 14, Oster Dow Jones Commodity News* — **USDA to send BSE delegation to Japan for talks. The U.S. Department of Agriculture (USDA) is planning to send Undersecretary for Farm and Foreign Agriculture Services J.B. Penn and others to Tokyo in August to meet with officials there in hopes of ending Japan's ban on U.S. beef, USDA spokesperson Ed Loyd said.** USDA Secretary Ann Veneman said Wednesday, July 14, she was encouraged by the fact that Japan and the U.S. are cooperating in an ongoing series of technical meetings on Japan's ban and the case of bovine spongiform encephalopathy (BSE) the U.S. discovered in December. She told U.S. lawmakers in the House of Representatives she is hopeful about the outcome. USDA Undersecretary J.B. Penn has told reporters twice in recent months that negotiations with Japan will likely result in beef trade resuming this summer. **Japan, which is traditionally the largest foreign market for U.S. beef, banned it in December after the USDA announced the discovery of a case of BSE.** The U.S. exported 352,448 metric tons of beef to Japan in 2003, worth about \$1.3 billion, according to USDA data compiled by the U.S. Meat Export Federation.

Source: http://www.agprofessional.com/show_story.php?id=26207

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

Water Sector

19. *July 14, Water Week* — **EPA adds training workshops. The U.S. Environmental Protection Agency (EPA) has added free training workshops for small and medium–size water utilities on emergency response planning (ERP) to the five it held in June.** Designed to cover EPA's recently released guidance on emergency response planning for small and medium–size water systems, the workshops also review the agency's Response Protocol Toolbox on planning for and responding to drinking water contamination threats as well as some other agency security tools such as an online compendium for selecting analytical labs for handling emergency response samples and the agency's security product guides. Participation is limited to individuals representing water utilities and their invited private–sector clients, water–sector associations, government officials, emergency service providers, and certain trainers.

Source: <http://www.awwa.org/communications/waterweek/index.cfm?ArticleID=338>

20. *July 14, Associated Press* — **Southland agency pushes desalting more seawater.** Southern California needs to turn more ocean water into drinking water as part of an updated plan to augment the region's supplies by 2025, leaders of the nation's largest urban water district said Tuesday, July 13. **The board of the Metropolitan Water District of Southern California adopted a revised plan that calls for increased seawater desalination and more water from Northern California over the next two decades.** About 18 million Southern Californians — roughly one of every two state residents — get their water from Metropolitan. **The additional supply would amount to an extra buffer of 500,000 acre–feet of water. That's enough water to supply 1 million households for a year.** Half the water would come from increased seawater desalination, water recycling, and groundwater. Increased storage and transfer from two massive water projects that ferry water from north to south — the State Water Project and the Central Valley Project — would supply the rest.

Source: <http://www.dailynews.com/Stories/0.1413,200~20954~2270360.00.html>

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

Public Health Sector

21. *July 15, Associated Press* — **Bill to develop bioterror vaccines sent to Bush. Lawmakers who experienced the dangers of anthrax firsthand sent President Bush legislation Wednesday, July 14, to give private companies \$5.6 billion in incentives to develop antidotes to biological and chemical weapons.** Over the next 10 years, the act would give the pharmaceutical industry the financial guarantees it says it needs to research and produce vaccines and antidotes for bioterror agents. With the House vote, Congress completed work on legislation Bush requested in a State of the Union speech 18 months ago. Agreement between the House and Senate was delayed by a dispute over how to guarantee a steady stream of funding to drug makers without taking away Congress's authority to make annual decisions on

spending levels. The legislation guarantees that any company that develops countermeasures to treat diseases and conditions caused by bioterrorism would have a buyer in the federal government. Also included would be antidotes for chemical, radiological, and nuclear agents. Source: http://www.boston.com/news/nation/articles/2004/07/15/congress_approves_56b_bioterror_bill/

22. *July 15, European Space Agency* — **Space technology captures toxic micro-organisms. Sophisticated technology developed to ensure clean air for astronauts onboard space stations is now used in hospitals to capture and destroy airborne fungi, bacteria, spores, and viruses. It can also eliminate microorganisms causing Severe Acute Respiratory Syndrome, ebola, smallpox, and tuberculosis as well as anthrax.** Most of the airborne micro-organisms around us do not present grave hazards to healthy people, however they can pose serious threats to those with reduced immune resistance. The technology is a multistage system using strong electric fields and cold-plasma chambers to eliminate micro-organisms in the air.
Source: http://www.esa.int/esaCP/SEMKAWL26WD_Improving_0.html

23. *July 14, Reuters* — **Drug-resistant germ spreading outside U.S. hospitals.** A drug-resistant "superbug" found in hospitals has a close cousin that is affecting athletes, prisoners, and small children in growing numbers across the U.S., disease experts said on Wednesday, July 14. Methicillin-resistant *Staphylococcus aureus* (MRSA) can become fatal if not treated with the right antibiotics, said Daniel Jernigan of the U.S. Centers for Disease Control and Prevention (CDC). **"MRSA is showing up in places it had never been seen before -- as a predominant cause of skin disease among children in some regions of the country, as clusters of abscesses among sports participants, as the most common cause of skin infections among inmates in some jails and among military recruits and rarely, as a severe and sometimes fatal lung or bloodstream infection in previously healthy people," Jernigan said.** Jernigan said studies have shown MRSA makes up a significant number of all diagnosed staph infections, ranging from nine percent in Maryland, to 20 percent in Georgia, and 30 percent in Hawaii. The numbers are rising, Jernigan said. "We also found that rates of community-associated MRSA infections were disproportionately higher among children," he said.
Source: <http://www.reuters.co.uk/newsArticle.jhtml?type=healthNews&storyID=5671334§ion=news>

24. *July 14, Voice of America* — **New York adds another weapon in fight against bioterrorism.** Almost three years after a series of anthrax attacks terrified New Yorkers, the city has opened a high security laboratory to detect bioterrorism threats. **The new \$16 million laboratory is designed to deal with a broad range of bioterror threats as well as infectious diseases.** In the past, New York had to use the U.S. Centers for Disease Control and Prevention in Atlanta, GA, to test pathogens and germs. Plans for a new high-tech lab, first made in 1992, languished for almost a decade. But the 2001 anthrax attacks and the city's inability to respond quickly and efficiently, led to the new laboratory which will employ more than 100 scientists and technicians. City Health Commissioner Thomas Frieden says the 1,858 square meter facility puts New York at the forefront in the study and prevention of infectious diseases such as AIDS, tuberculosis, and the West Nile virus.
Source: <http://www.voanews.com/article.cfm?objectID=A3749686-B780-41>

25. *July 14, Argonne National Laboratory* — **Scientists determine structure of staph, anthrax enzyme. Researchers at the U.S. Department of Energy's Argonne National Laboratory and the University of Chicago have determined the crystal structure of sortase B, an enzyme found in the bacteria that cause staph and anthrax. While an antibiotic is probably five to seven years away, the structure could provide the first clue in developing a treatment for the infections.** By analyzing genomes, the researchers uncover information that will lead to structure-based or "rational" drug design. The problem is that researchers don't know what half the proteins coded by the genome do or how they work. Now that the researchers understand the enzyme, they hope to find a way to stop it -- or at least to slow it down. Sortase attaches proteins to the surface of bacterial pathogens. These proteins help the pathogens survive and flourish. Bacteria like staph and anthrax need iron to function. But little free iron is available in the blood stream because most of it is bound in red blood cells. So the bacteria develop a mechanism to pry open the red blood cells, and these proteins help them. The research is published in the journal *Structure*.

Source: http://www.eurekalert.org/pub_releases/2004-07/dnl-asd071404.php

26. *July 13, Food and Drug Administration* — **Tests of prescription drugs from bogus Canadian Website show products are fake. A Food and Drug Administration (FDA) analysis of three prescribed drugs purchased from a Website advertised as Canadian showed that the drugs bought were fake, substandard and potentially dangerous. One was a controlled substance.** FDA investigators recently purchased three commonly prescribed drugs from a Website advertising "Canadian Generics," which had been sending "spam" e-mails promoting its products. The products purchased were so-called "generic" versions of Viagra, Lipitor, and Ambien. None of the three products has a U.S.-approved generic version, and so all three drugs were unapproved. "The test results of our analyses offer proof positive that buying prescription drugs online from unknown foreign sources can be a risky business. As was the case here, even where a Website looks legitimate, FDA has clear evidence that the Website is dispensing misbranded drugs that are not the same quality as those approved by the FDA for sale in the United States," said FDA Acting Commissioner Lester M. Crawford.

Source: <http://www.fda.gov/bbs/topics/news/2004/NEW01087.html>

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

Government Sector

Nothing to report.

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

Emergency Services Sector

27. *July 15, Boston Globe* — **High-tech security gear unveiled for convention. Security officials are deploying more than a half-dozen mobile command vehicles around Greater Boston, MA, during the Democratic National Convention to ensure that communication among law enforcement and rescue agencies continues in the event of a terrorist attack.**

Security officials will be using a wide range of space-age technologies. Robots operated by suitcase-sized remote controls will check out suspicious packages, building-top security cameras will zoom in to read license plate numbers, and some security officers will carry hand-held computers that can receive photos of suspicious persons and other images that could be helpful in preventing or responding to an attack. Speaking to reporters, Department of Homeland Security Secretary Tom Ridge listed a series of extraordinary steps being taken to guarantee security during the convention, including round-the-clock video surveillance in parts of downtown Boston, the X-raying of shipments going to the convention arena, and the use of a record number of bomb-sniffing dogs. **If communications are knocked out at the convention's main security operations center, the approximately 35 agencies involved with convention security would be able to stay in close contact with videoconferencing and secure camera feeds available in the mobile command vehicles.**

Source: http://www.boston.com/news/local/massachusetts/articles/2004/07/15/high_tech_security_gear_unveiled_for_convention/

[[Return to top](#)]

Information Technology and Telecommunications Sector

28. July 14, e-matters — PHP memory_limit remote vulnerability. PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. According to Security Space PHP is the most popular Apache module and is installed on about 50% of all Apaches worldwide. This figure includes of course only those servers that are not configured with `expose_php=Off`. During a reaudit of the `memory_limit` problematic **it was discovered that it is possible for a remote attacker to trigger the memory_limit request termination in places where an interruption is unsafe. This can be abused to execute arbitrary code on remote PHP servers.** It is strongly recommended that users running PHP with compiled in `memory_limit` support upgrade as soon as possible to the newest version.

Source: <http://security.e-matters.de/advisories/112004.html>

29. July 14, IDG News Service — Voice over IP has FCC ally. Congress probably won't act on pending bills to clarify Voice over IP (VoIP) technology regulation in the current session, but Federal Communications Commission (FCC) Chairman Michael Powell hopes to make progress on the issue this year. Powell made his comments at the Always On Network LLC's AO2004 conference at Stanford University in Palo, Alto, CA, this week. **The question whether VOIP should be treated as a telephone service or an information service has implications for taxation as well as issues such as 911 emergency call services and wiretapping.** An FCC public comment period on VOIP closed Wednesday, July 14. The agency expects to look at the comments and make some decisions on the issue by the end of this year, though some aspects of VoIP regulation, such as how much a carrier must pay to terminate a call, may not be settled for years, FCC policy chief Robert Pepper says. Congressional action is the surest way to clarify VoIP regulation, Powell said. The FCC can take bold action but can also be sued under the claim that its moves violate the Telecommunications Act of 1996, he noted. Another VOIP battleground is in state governments, which have fiercely resisted giving up their traditional telecommunications taxes and regulations when it comes to VoIP, Powell said. **States should not regulate VOIP, at**

least in terms of economic issues such as pricing, Powell said.

Source: <http://www.pcworld.com/news/article/0,aid,116905,00.asp>

30. *July 12, SecurityFocus* — **Microsoft Outlook Express message window script execution vulnerability.** Microsoft Outlook Express is reported prone to a vulnerability that may allow unauthorized execution of script code. It is reported that **Outlook Express filters user-supplied input such as script code in the 'window.document' object, however, it fails to filter script code in any other components of the window object. This may aid in attacks that occur through HTML e-mail.** Microsoft Outlook Express version 6.0 is currently known to be vulnerable to this issue, however, it is possible that other versions are affected as well. Currently, SecurityFocus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/10692/info/>

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: Microsoft has released its July Security Updates. Two of these updates are of a critical nature and should be applied to vulnerable systems. For more information, see Microsoft's bulletin at http://www.microsoft.com/security/bulletins/200407_windows.m_spx	
Current Port Attacks	
Top 10 Target Ports	9898 (dabber), 5554 (sasser-ftp), 445 (microsoft-ds), 137 (netbios-ns), 1023 (Reserved), 135 (epmap), 1434 (ms-sql-m), 4899 (radmin), 1433 (ms-sql-s), 3127 (mydoom)
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

31. *July 14, PR Newswire* — **ATF national response team activated in Pottstown fire. A National Response Team (NRT) from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) arrived in Pottstown, PA, on Wednesday, July 14, to assist in the investigation of a fire of unknown origin that engulfed a three-story building housing the Topos Mondial Corporation.** The fire, which occurred Tuesday, July 13, at a commercial building at the intersection of Queen and South Adams Streets in Pottstown, is estimated to have caused damage in excess of \$1 million. Although the NRT has been used primarily to

assist in the investigation of suspicious commercial fires, it has also been activated to the scenes of criminal bombings such as the Oklahoma City bombing and the 1993 World Trade Center bombing, and explosions at explosives and ammunition manufacturing plants, legal fireworks factories, and illegal explosive device manufacturing operations. Other agencies involved in this investigation are the Montgomery County, PA, District Attorney, the Pennsylvania State Police, and the Pottstown Police and Fire departments.

Source: [http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=
/www/story/07-14-2004/0002210555&EDATE=](http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/07-14-2004/0002210555&EDATE=)

[[Return to top](#)]

General Sector

Nothing to report.

[[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 page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

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

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – 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.

[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:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.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 soc@us-cert.gov or visit their Web page at www.us-cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report 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.