



Department of Homeland Security

IAIP Directorate

Daily Open Source Infrastructure Report for 21 September 2004

Current Nationwide Threat Level is



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

www.whitehouse.gov/homeland

Daily Overview

- The Department of Transportation has announced grants to states, territories and Native American tribes totaling \$12.8 million for planning and training to improve response to hazardous materials transportation incidents. (See item [4](#))
- Reuters reports researchers are predicting that super drug-resistant forms of tuberculosis are at the tipping point of a global epidemic, and only small changes are needed to help them spread quickly. (See item [19](#))

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. *September 20, Associated Press* — **U.N. official: 40 nations can make nukes.** More than 40 countries with peaceful nuclear programs could retool them to make weapons, the head of the U.N. atomic watchdog agency said Monday, September 20, amid new U.S and European demands that Iran give up technology capable of producing such arms. **Mohamed ElBaradei, director general of the International Atomic Energy Agency (IAEA), suggested in a keynote address to the IAEA general conference that it was time to tighten world policing of nuclear activities and to stop relying on information volunteered by countries.** Beyond the declared nuclear arms-holding countries, "some estimates indicate that 40 countries or more now have the know-how to produce nuclear weapons," ElBaradei said. "We are relying primarily on the continued good intentions of these countries, intentions, which ... could ... be

subject to rapid change." **His comments appeared prompted by a series of revelations of proliferation or suspected illicit nuclear activities over the past two years.** ElBaradei did not name the countries capable of quickly turning peaceful nuclear activities into weapons programs. **But more than a dozen European countries with either power-producing nuclear reactors or large-scale research reactors are among them, as well as Canada, and countries in Asia, Africa and Latin America.**

Source: <http://www.nytimes.com/aponline/international/AP-Nuclear-Age.ncy.html>

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

Chemical Industry and Hazardous Materials Sector

Nothing to report.

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

Defense Industrial Base Sector

Nothing to report.

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

Banking and Finance Sector

2. *September 20, Information Week* — **More security attacks motivated by greed, Symantec reports.** The Internet security company Symantec Corporation on Monday, September 20, released its Internet Security Threat Report, which provides a six-month snapshot of security events the vendor monitored for the first six months of 2004. The reports states, among other things, that there has been an increase in profit-motivated attacks, according to Vincent Weafer, senior director of Symantec's virus research team. **The security company is reporting that attacks aimed at E-commerce sites rose from 4% of overall attacks to 16%. Other trends that point to attacks for profit include the increase in phishing scams and spyware designed to pilfer user names, passwords, and financial information,** Weafer says.
Source: <http://www.informationweek.com/story/showArticle.jhtml?artic leID=47900343>

3. *September 20, PR Newswire* — **U.S. financial institutions to increase budgets and training to combat money laundering.** U.S. financial institutions will continue to spend at a brisk pace to combat money laundering over the next three years, with some banks expecting costs to more than double during the period, according to a new survey by audit, tax and advisory firm KPMG LLP. **The survey indicates that costs will rise, in part, because of transaction monitoring required by federal law and and a desire to thwart terrorism globally,** according to Ellen Zimiles, a partner in KPMG's Forensic practice. "Because this is a matter of both regulatory compliance and homeland security, U.S. financial institutions are heeding a clear message: Be more accountable or risk stiff consequences," she said. "Perhaps the biggest challenge for U.S. financial institutions is to install a more accountable anti-money laundering system without imposing upon and diluting service to clients and potential customers," Zimiles said. Zimiles added that it is encouraging to see a majority of financial-services institutions, especially upper management, embrace their anti-money laundering responsibilities. **Officials**

at both the International Monetary Fund and The United Nations Office of Drug Control Prevention estimate that between \$500 billion and \$1 trillion in funds is laundered worldwide annually by drug dealers, arms traffickers, terrorists and other criminals.

Source: <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/09-20-2004/0002253528&EDATE=>

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

Transportation Sector

4. *September 20, Department of Transportation* — **DOT awards \$12.8 million in Hazmat grants.** Department of Transportation (DOT) Secretary Norman Y. Mineta on Monday, September 20, **announced grants to states, territories and Native American tribes totaling \$12.8 million for planning and training to improve response to hazardous materials transportation incidents.** DOT's Research and Special Programs Administration (RSPA) made the funds available under the Hazardous Materials Emergency Preparedness (HMEP) Grants Program. The HMEP grants support the development of emergency response strategies tailored to regional needs and are funded through registration fees paid by shippers and carriers of certain hazardous materials. More than one million emergency responders, as well as 3,000 local emergency planning committees from across the nation, have received training and support under HMEP since the program began in 1993. The six largest grants were awarded to California, \$964,316; Texas, \$668,460; Illinois, \$612,982; Ohio, \$510,751; New York, \$470,968; and Florida, \$453,407.
Source: <http://www.dot.gov/affairs/rspace604.htm>
5. *August 20, Government Accountability Office* — **GAO-04-901: Air Traffic Control: System Management Capabilities Improved, but More Can Be Done to Institutionalize Improvements (Report).** Since 1981, the Federal Aviation Administration (FAA) has been working to modernize its aging air traffic control (ATC) system. Individual projects have suffered cost increases, schedule delays, and performance shortfalls of large proportions, leading the Government Accountability Office (GAO) to designate the program a high-risk information technology initiative in 1995. Because the program remains a high risk initiative, GAO was requested to assess FAA's progress in several information technology management areas. This report, one in a series responding to that request, has two objectives: (1) to evaluate FAA's capabilities for developing and acquiring software and systems on its ATC modernization program, and (2) to assess the actions FAA has under way to improve these capabilities. **GAO is making recommendations to the Secretary of Transportation to address specific weaknesses and to institutionalize FAA's process improvement initiatives by establishing a policy and plans for implementing and overseeing process improvement initiatives.** In commenting on a draft of this report, agency officials generally agreed with GAO's recommendations. Highlights: <http://www.gao.gov/highlights/d04901high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-901>
6. *August 20, Government Accountability Office* — **GAO-04-822: Information Technology: FAA Has Many Investment Management Technologies in Place, but More Oversight of Operational Systems Is Needed (Report).** The Federal Aviation Administration's (FAA) mission is to promote the safe, orderly, and expeditious flow of air traffic in the United States

airspace system, commonly referred to as the National Airspace System (NAS). To maintain its ability to effectively carry out this mission FAA embarked, in 1981, on a multibillion dollar effort to modernize its aging air traffic control (ATC) system, the principle technology component of the NAS. To gain insight into how FAA is meeting its management challenges, congressional requesters asked the Government Accountability Office (GAO) to evaluate FAA's processes for making IT investment management decisions. The objectives of this review included (1) evaluating FAA's capabilities for managing its IT investments, and (2) determining what plans, if any, the agency might have for improving these capabilities. **To strengthen FAA's investment management capability, GAO recommends that FAA develop and implement a plan to address the weaknesses identified in this report.** In commenting on a draft of this report, the Department of Transportation commented that the report was balanced and fair, showing where FAA has many capabilities in place and identifying areas that need improvement. Highlights:

<http://www.gao.gov/highlights/d04822high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-822>

[[Return to top](#)]

Postal and Shipping Sector

7. *September 20, DM News* — **World postal volume dips. Despite slight decreases in worldwide letter and parcel volumes from 2002 to 2003, public postal operators remain optimistic that their strategies will bring mail volume growth over the next five years, according to a report from the Universal Postal Union during its 23rd Congress in Bucharest, Romania.** While electronic substitution continues to affect worldwide letter volumes, e-commerce development is expected to generate greater parcel volumes in the future. As a result, many public postal operators are implementing logistics and online services to respond to customers' needs. The report, "Postal Market 2004: Review and Outlook," shows postal sector developments from 1998 to 2003. It includes public postal operators' predictions for the period up to 2008. Worldwide domestic letter volumes totaled 424 billion pieces in 2003, down 0.4 percent from 2002. Except for some industrialized countries and countries in the Asia/Pacific region, public postal operators in most regions predict higher domestic letter volumes through 2008. Worldwide international letter volumes exceeded six billion pieces in 2003, down 5.1 percent from 2002. The drop affected almost three-quarters of all countries. International letter volumes represented 1.4 percent of worldwide volume in 2003 versus two percent in 1995.

Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=30438

[[Return to top](#)]

Agriculture Sector

8. *September 20, USAgNet* — **Grain elevator explosion.** Two men remain in critical condition at a Lubbock, TX, hospital, after being injured in an explosion in Lazbuddie. It happened Friday, September 17, at the A.G.P. Grain Elevator in Lazbuddie. The state's fire marshal is investigating just how the grain elevator exploded. It appears to be a gas leak that caused an

explosion in the control room.

Source: <http://www.usagnet.com/story-national.cfm?Id=979&yr=2004>

9. *September 18, Ledger (FL)* — **Commercial citrus acreage drops. Development, disease, and a declining market for Florida citrus products has led to the largest loss of commercial citrus acreage during the past two years than in any similar period not affected by a freeze.** Florida's citrus land dropped to 748,555 acres this year, a loss of 6.1 percent of commercial acres since 2002, according to the biennial Commercial Citrus Inventory released by the Florida Agricultural Statistics Service, part of the U.S. Department of Agriculture (USDA). The inventory was completed in July before hurricanes Charley and Frances struck the state's citrus belt. The USDA agency will not resurvey the hurricane-damaged areas until the next inventory in two years. Commercial citrus acreage last peaked in 1996 and has been declining ever since at an accelerating pace. The state lost more than 12,000 acres in the 1998 and 2000 inventories and 34,972 acres in the 2002 census. Economic pressures mean growers are not replanting when they lose groves to disease, particularly the fatal citrus Tristeza virus, said Richard Kinney, the chief executive at Florida Citrus Packers in Lakeland, which represents most of the state's fresh citrus shippers. The virus is expected to wipe out tens of thousands of trees over the next decade.

Source: <http://www.theledger.com/apps/pbcs.dll/article?AID=/20040918/NEWS/409180342/1178>

[[Return to top](#)]

Food Sector

10. *September 20, Associated Press* — **Beef recalled. Packerland Packing Co. has recalled 59,000 pounds of ground beef sold in seven states that may be contaminated with E. coli bacteria. The beef was produced at Packerland's Green Bay, WI, facility, and was distributed to stores in Illinois, Indiana, Louisiana, Massachusetts, South Carolina, Virginia, and Wisconsin.** Stores were asked to remove the product. Steve Van Lannen, general manager for the company, said in a statement the company was working with the U.S. Department of Agriculture. Packerland recalled the meat after its internal testing showed the ground beef was possibly contaminated and mistakenly shipped.

Source: <http://msnbc.msn.com/id/6053675/>

11. *September 20, Medical News Today* — **Outbreak of Cyclosporiasis.** During June and July 2004, public health officials in Pennsylvania were notified of cases of the parasitic disease cyclosporiasis (1,2) among persons associated with a residential facility. The U.S. Centers for Disease Control and Prevention (CDC) confirmed the diagnosis of *Cyclospora cayentanensis* infection (1) by examining stool specimens from multiple patients. By early July, local public health officials had been notified of approximately 50 potential cases of cyclosporiasis associated with the facility. **Epidemiologic and traceback investigations determined the cases were linked to consumption of raw Guatemalan snow peas at five special events, for which food was prepared by the facility staff, from late May through late June.** This is the first documented outbreak of cyclosporiasis linked to snow peas. The Food and Drug Administration (FDA) and CDC are working with Guatemalan officials to determine the sources of the snow peas and possible modes of contamination.

Source: <http://www.medicalnewstoday.com/medicalnews.php?newsid=13631>

12. *September 18, Associated Press* — **Pork pulled off shelves to check for metal devices. More than a thousand pounds of pork processed at a Sioux, IA, meatpacking plant was recalled Saturday, September 18, because a microchip could be embedded in the meat.** The Sioux–Preme Packing Co. recalled 110 pork shoulder butts — about 1,100 pounds of meat — that could contain the metal devices used to measure scientific data in hogs. The animals, processed September 10, were part of a research herd that had been sent to slaughter without the proper notification that they had the chips implanted, said Sioux–Preme Vice President Jim Malek. The meat had been sent to processors in Colorado, Iowa, and Mexico. None of the meat appeared to have reached consumers, Malek said. Recipients were notified to return meat, which will either be reinspected and cleared for use or destroyed, Malek said. Malek said he didn't know who had implanted the chips in the hogs but the hogs were healthy and had been cleared by the U.S. Department of Agriculture inspectors for processing.

Source: <http://www.cnn.com/2004/US/09/18/pork.recall.ap/index.html/>

13. *September 02, Agricultural Research Service* — **Free–range chicken no guarantee. There is no discernible difference in Salmonella levels between free–range, organically produced poultry and conventionally produced birds, an Agricultural Research Service (ARS) scientist has found.** ARS microbiologist J. Stan Bailey of the Poultry Microbiological Safety Research Unit examined 110 processed free–range chickens from three organic producers and found that about 25 percent of the chickens tested positive for Salmonella. Chickens raised conventionally had about the same levels. Thus, the decision to purchase free–range chickens shouldn't be based on the belief that such a chicken is microbiologically superior, according to Bailey.

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

[[Return to top](#)]

Water Sector

14. *September 20, Atlanta Journal Constitution (GA)* — **Sewage runs into Nancy Creek. Northwest Atlanta, GA, residents breathed fumes from 10 million gallons of raw sewage floating in Nancy Creek during the weekend after a wastewater line ruptured under the severe flooding from Hurricane Ivan.** A replacement pipe was installed on Sunday, September 19, but city officials could not predict when the pollution, which had reached several miles downstream to the Chattahoochee River, would clear. In the meantime, they warned against fishing or entering the creek or the Chattahoochee for several days. The sewer system and the city's drinking water were unaffected. Workers will be installing devices in the creek to slow the flow of filth downstream. The vestiges of last week's Hurricane Ivan possessed the lingering force to yank the concrete pipe, four feet wide and weighing more than two tons, from the embankment just north of West Paces Ferry Road.

Source: http://www.ajc.com/metro/content/metro/atlanta/0904/20nancys_ewage.html

15. *September 18, Seattle Post Intelligencer (WA)* — **E. coli in school's drinking water. Students and staff at Kendall Elementary School in Whatcom, WA, are being warned not to drink**

the school's tap water after testing discovered E. coli bacteria in the drinking water, according to the state health department. Bottled water is being provided to the school's 640 students and staff until officials can confirm all traces of E. coli are gone. The water system has been disinfected and inspected by the health department, and a sample will be tested again early next week, according to the health department. Water for the school, located in a rural area of the county, comes from its own well.

Source: http://seattlepi.nwsourc.com/local/191444_ecoli18.html

16. *September 15, Water Week* — **WSCC to begin organizing. The 24-member Water Sector Coordinating Committee (WSCC) established by the Department of Homeland Security (DHS) will conduct its initial organizing meeting September 28–29.** To be self directed and maintained, the panel of water and wastewater community interests is to help DHS implement Homeland Security Presidential Directive 7 (HSPD7), which is intended to bolster the security of various critical infrastructure sectors. The primary objective of the WSCC, meetings of which will not be open to the public, is to help coordinate programs and facilitate communication and information sharing both within the sector and among DHS, USEPA and other infrastructure sectors. The panel's first meetings are being managed, under contract with DHS, by the George Mason University Critical Infrastructure Protection Project.

Source: <http://www.awwa.org/communications/waterweek/index.cfm?ArticleID=360>

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

Public Health Sector

17. *September 20, Kyodo News* — **Japan is largest exporter of measles.** Japan is the largest exporter of measles to the U.S., according to a Centers for Disease Control and Prevention (CDC) study. **The study, published by the Journal of Infectious Diseases, found that the cases of measles brought to the U.S. from Japan over a nine-year period to 2001 accounted for 15 percent of the total number of imported cases of measles contracted outside the U.S.** Acting on this, the CDC has sought help from Japan and other countries to address the problem, saying U.S. efforts alone cannot eradicate it. Researchers say Japan's status as a major exporter of measles reflects the large number of people traveling between Japan and the U.S. — the count in 2002 estimated at 4.3 million — in addition to sporadic measles outbreaks in Japan.

Source: <http://www.japantoday.com/e/?content=news&cat=1&id=312691>

18. *September 20, Progress Index (VA)* — **More than nine hundred workers in Virginia have had smallpox vaccine.** Across the state health care workers and emergency response personnel are now a little more prepared for the possibility of a smallpox attack according to the Virginia Department of Health. **A select group of 913 people across the state were vaccinated, which includes, 353 public health staff, 415 hospital staff, and 145 other emergency responders according to a press release from the Virginia Department of Health.** "Virginia now has a core group of healthcare personnel and other responders throughout the state prepared to rapidly respond in the event a case of smallpox disease should ever occur," said State Health Commissioner Robert B. Stroube. Lee explained that the state will continue to provide the vaccine upon request to volunteer healthcare personnel, or emergency responders, although fulfilling such requests will be determined based on careful consideration of vaccine

management issues. Each vial of smallpox vaccine contains 100 doses and expires within 90 days after being mixed. The handling of the vials is sensitive due to temperature control requirements.

Source: http://www.zwire.com/site/news.cfm?newsid=12961263&BRD=2271&PAG=461&dept_id=462946&rfti=6

19. *September 19, Reuters* — **TB set to be global scourge again. Super drug-resistant forms of tuberculosis (TB) are at the tipping point of a global epidemic, and only small changes are needed to help them spread quickly, researchers predicted Sunday, September 19.** Two separate studies show that multiple-drug-resistant TB, which can only be cured with a carefully monitored cocktail of drugs taken for months on end, could easily start spreading more commonly. The reports, to be published in the journal *Nature Medicine*, coincide with another report published last week saying the World Health Organization's efforts to control multi-drug-resistant TB were not working as well as hoped. If all the reports are true, it means that TB could make a dangerous new resurgence, and with new strains that are even harder to fight than the old ones. TB infects an estimated 8.7 million people a year and kills two million a year despite widespread control efforts. Tough hygiene and treatment campaigns beat TB back in places such as Europe and North America, but AIDS, with its attacks on the immune system, helped TB make a comeback in the 1990s. TB is making special gains in Eastern Europe and Southeast Asia. And TB strains resistant to several antibiotics are becoming increasingly prevalent, with "hot spots" in Russia, Eastern Europe, South Africa, China, and Israel.
- Source: <http://www.reuters.com/newsArticle.jhtml?type=healthNews&storyID=6273329>

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

Government Sector

Nothing to report.

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

Emergency Services Sector

20. *September 20, Chicago Sun Times (IL)* — **Firefighters face intense training.** Nearly one year after mistakes by the Chicago Fire Department contributed to six deaths at a Loop high-rise fire, Fire Commissioner Cortez Trotter on Monday, September 20, unveiled sweeping changes aimed at making certain it never happens again. **Increased training, annual physical fitness testing for veteran firefighters and a new general order that will serve as the playbook during high-rise fires are the cornerstones of reforms made in response to a scathing report by the Mikva Commission.** Chicago firefighters have been conducting top-to-bottom stairway searches ever since the October 17 fire at 69 W. Washington, when there was a 90-minute gap between the time firefighters arrived on the scene and the time the bodies of six victims were found. "We have identified and assigned personnel strictly for search-and-rescue operations. They will not be assigned to firefighting operations. They will be specifically assigned to search and rescue — top-to-bottom. That's their exclusive duty. I've given them a specific title and assignment," Trotter said. The Fire Department has already sent 75 top brass back to school for eight-hour classes in the nearly five months since Trotter took over.

"Although fires are down and high-rise fires are rarities, only with continued education and continued training can we be ready to fight these fires," Trotter said.

Source: <http://www.suntimes.com/output/news/cst-nws-fire20.html>

21. *September 20, USA TODAY* — **FEMA team arrives on heels of hurricane.** As Hurricane Ivan took its deadly swipe at Pensacola, FL, last week, the Federal Emergency Management Agency (FEMA) was mobilizing a team of 31 doctors, nurses and paramedics in Jacksonville, 350 miles away. Just hours after Ivan struck on Thursday, September 17, the medical team set out in a convoy across the Florida Panhandle, escorted by the state highway patrol. The mobile emergency crew — called a Disaster Medical Assistance Team by FEMA — also demonstrates the "new" FEMA that has emerged since the 9/11 terrorist attacks. **Since FEMA was folded into the Department of Homeland Security in March 2003, the agency's role has expanded to providing a direct response to a disaster — whether in the form of medical care or emergency supplies — as well as aiding in the recovery to rebuild homes and businesses.** The Jacksonville-area FEMA medical team convoy had two 20-foot trucks and eight rented vans. The workers immediately began setting up a triage tent, a medical tent, a pharmacy, a command center and a sleep tent.

Source: http://www.usatoday.com/news/nation/2004-09-20-fema-florida_x.htm

22. *September 20, Westerly Sun (RI)* — **Drill focuses on chemical spill. A mock hazardous material spill drew more than 100 firefighters and rescue personnel from several Connecticut and Rhode Island departments to the Yardney Technical Products battery plant in Pawcatuck, RI, on Sunday, September 19, creating the town's largest chemical emergency drill ever conducted.** "We weren't training for a certain hazardous material. The effort was to train for mutual aid services," said Pawcatuck Fire Chief Kevin Burns. The Yardney plant, which develops specialty batteries, such as the Lithium ion ones that NASA used earlier this year in the Spirit Mars rover, was selected to house the drill mostly due to its location near the Rhode Island border, said Burns. Ambulances from eight Connecticut and Rhode Island towns transported the mock Boy Scout victims to the Westerly Hospital from the plant, which employs about 170 people. While town firefighters routinely train for hazardous material emergencies, Sunday's drill allowed them to prepare for a chemical spill on a much larger scale than they are used to.

Source: <http://www.thewesterlysun.com/articles/2004/09/20/news/news1.txt>

23. *September 20, Department of Transportation* — **DOT awards \$250,000 to International Association of Fire Fighters for Hazmat response training.** On Monday, September 20, Department of Transportation (DOT) Secretary Norman Y. Mineta announced a \$250,000 federal grant to the International Association of Fire Fighters (IAFF) **to provide vital training resources for instructors who conduct hazardous materials response training programs.** The grant to IAFF pays instructor salaries, travel, training books and classroom materials for the hazardous materials instructor courses, which are scheduled annually across the country. The U.S. Department of Transportation's Research and Special Programs Administration (RSPA) made the funds available under the Hazardous Materials Emergency Preparedness (HMEP) Grants Program. Since issuing the first HMEP grant in 1993, the program has provided more than \$112 million in grants to train 1,587 fire service instructors. The instructors, in turn, used their training to teach another 1,546,412 Hazmat responders.

Source: <http://www.dot.gov/affairs/rspa504.htm>

Information Technology and Telecommunications Sector

24. *September 20, Secunia* — **xine-lib multiple buffer overflow vulnerabilities.** Multiple vulnerabilities have been reported in xine-lib, which can be exploited by malicious people to compromise a user's system. The vulnerabilities have been fixed in version 1-rc6a:
<http://xinehq.de/index.php/releases>
Source: <http://secunia.com/advisories/12602/>
25. *September 20, CNET News.com* — **Viruses keep on growing. The volume of worms and viruses is increasing, but the rate of successful attacks has dropped, according to a new report from Symantec.** The antivirus company's biannual Internet Security Threat Report found that 4,496 new Windows viruses and worms were released between January and June, up more than 4.5 times from same period last year. But overall, Symantec, the daily volume of actual attacks decreased in the first six months of 2004. Alfred Huger, a senior director at Symantec's Security Response team said malicious code writers were increasingly going to spammers to sell them access to the computers that they hack, or break into. Spammers, after paying the hackers, then flood those hacked computers with unsolicited messages, or spam. **Symantec also said it expects more viruses and worms in the future to be written to attack systems that run on the Linux operating system and hand-held devices as they become more widely used.** The report also noted that the rate at which personal computers are being hijacked by hackers rocketed in the first half of 2004. An average of 30,000 computers per day were turned into enslaved "zombies," compared with just 2000 per day in 2003. Report: <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>
Source: http://news.com.com/Viruses+keep+on+growing/2100-7349_3-5374399.html?tag=nefd.top
26. *September 20, Secunia* — **Sun Java Enterprise System NSS library vulnerability. Sun has acknowledged a vulnerability in the NSS library included with Sun Java Enterprise System.** This vulnerability was originally reported on August 25 and is caused due to a boundary error within the parsing of records during SSLv2 connection negotiation. The vulnerability can be exploited to cause a heap-based buffer overflow by sending a specially crafted client hello message with an overly long record. Successful exploitation allows execution of arbitrary code with the privileges of an application linked to the vulnerable library. Original advisory and workaround:
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57643-1>
Source: <http://secunia.com/advisories/12599>
27. *September 19, Jerusalem Post (Israel)* — **Algorithms can identify cyber-terrorism.** Professor Mark Last of the Ben-Gurion University (BGU) department of information systems engineering is working on ways to make terrorist's communication on the Internet more difficult by conducting pioneering research on fighting terror in cyberspace. "The Internet helps terrorists a great deal, and makes their life easier in many senses — because it is really a very difficult problem to find something suspicious in the sea of traffic. Access to the Internet is relatively easy and affordable worldwide, and it is easy to use while concealing your identity,"

Professor Last says. **His team has developed an experimental system that succeeded in identifying about 95% of Web pages with a terrorist content.** Last's cooperation with colleagues at the University of South Florida led to the U.S. National Institute of Systems Test and Productivity in Florida getting involved in the subject. His lab is now working as a subcontractor for the National Institute to design methods that will enable government agencies and commercial companies to improve security, quality and cost effectiveness of large-scale information systems, with a focus on cyber-terror. **Their ability to distinguish cyber-terror activity from normal activity is becoming increasingly more reliable thanks to changes in the algorithms.**

Source: <http://www.jpost.com/servlet/Satellite?pagename=JPost/JPArticle/ShowFull&cid=1095565998846>

28. *September 17, eWeek* — **DHS follows industry lead on cyber-terror.** Lawrence Hale, deputy director of the Department of Homeland Security's (DHS) cyber security division, said Friday, September 17, that the DHS depends on the private sector to take the lead in fighting cyber-terrorist threats. "The normal things you do to protect your network will help protect you against cyber-terrorism," he said. Speaking at a conference on cyber-security organized by NBC News and the Northern Virginia Technology Council, Hale said the department is already aware of some cyber-terror threats, as well as the activities of terrorist organizations on the Internet. "They're using cyberspace for recruiting, fund-raising and communication," he said. **Private-sector businesses in the United States are already taking the lead in making sure that they are protected against attacks and intrusion, according to Hale -- and the government is following their lead.** While he wouldn't divulge details, Hale said the government is working to lessen the severity of any attack on it. **He said the fact that most federal departments and agencies design and build their own networks and computer systems makes it less likely that any one type of attack would succeed across the government.** He also explained that the department wants to expand its role with private businesses in its fight against cyber terrorism.

Source: <http://www.eweek.com/article2/0,1759,1647410,00.asp>

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 released a new security bulletin detailing critical vulnerabilities in the way it handles JPEG graphics. More information can be found here: http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx .	
Current Port Attacks	
Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 137 (netbios-ns), 9898 (dabber), 5554 (sasser-ftp), 1434 (ms-sql-m), 1023 (Reserved), 80 (www), 4899 (radmin), 8000 (irdmi)

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

29. *September 20, Associated Press* — **Security guard shot at state Capitol. An unarmed security guard was shot just inside the Illinois state Capitol entrance Monday afternoon, September 20, and authorities are searching for the shooter, who fled the scene.** The shooter entered the north entrance and shot the security guard at about 1:45 p.m., then escaped in a vehicle, said Randy Nehrt, a spokesperson for the Secretary of State's Office, which has law enforcement jurisdiction over the building. Governor Rod Blagojevich was not in the Capitol at the time, and the Legislature is not in session. **The Capitol entrance has no metal detectors, and its law enforcement officers are not armed.** The Capitol was locked down for about an hour, following an announcement over the intercom ordering everyone to stay in their offices. Outside, police cars and ambulances surrounded the building, and officers roped off the entrance. After the lockdown was lifted, everyone entering the building was required to sign in, rather than the usual procedure of simply showing a badge to enter.

Source: <http://www.chicagotribune.com/news/local/chi-040920capitol.03826344.story?coll=chi-newsbreaking-hed>

[[Return to top](#)]

General Sector

30. *September 18, Interfax* — **Russian official does not rule out international terrorists obtaining nuclear materials.** "Today, we have to admit that we cannot fully rule out the possibility that fissile materials, including highly-enriched uranium and plutonium, as well as technologies suitable for manufacturing nuclear weapons may fall into the hands of international terrorists," the chief of the Russian Federal Nuclear Power Energy Alexander Rumyantsev said at an international conference of the Global Threat Reduction Initiative's partners in Vienna on Saturday, September 18. There are numerous international agreements that set safeguards requirements to materials and equipment, which helps lower the risk of fissile materials and nuclear explosive substances falling into the hands of terrorists, Rumyantsev said. **Nonetheless, he went on, "Actual situations have been reported in various countries where nuclear and radioactive materials have been stolen."** Rumyantsev continued, "A recent inspection operation carried out by the International Atomic Energy Agency has uncovered a diversified and highly-organized clandestine network engaged in illegally selling nuclear materials and technologies."

Source: http://cnniw.yellowbrix.com/pages/cnniw/Story.nsp?story_id=57283642&ID=cnniw&scategory=Energy:Nuclear&

[[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.