



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 31 July 2003

Current Nationwide Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports the TSA is seeking approval from Congress to cut \$104 million from the air marshal program to help offset a \$900 million budget shortfall, possibly cutting several thousand jobs. (See item [6](#))
- The New York Times reports legislation pending in the Senate would exempt some model-rocket propellants from toughened restrictions on explosives that were imposed by Congress last year. (See item [19](#))
- The Department of Homeland Security has updated the advisory "Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems." (See item [22](#))

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. ***July 29, Reuters*** — Arizona Palo Verde 3 nuke seen down for several days. The 1,270 megawatt Unit 3 at the Palo Verde nuclear power plant in Arizona is expected to be down for several more days according to a spokesperson for Arizona Public Service (APS), operator of the facility. The unit, along with other Arizona power plants, tripped off line Monday, July 28, due to an electrical problem related to work performed in the area by another

Arizona utility, Salt River Project. The other Arizona plants include two units at the Redhawk gas-fired plant, each around 530 MWs, and the 500 MW Unit 5 at the West Phoenix gas-fired plant. Those plants are back in service. The APS spokesperson said the delay in returning the nuclear unit was caused by the discovery of a small leak in a seal in a reactor coolant pump.

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=4023637

2. *July 29, Reuters* — **PSEG'S New Jersey Salem 1 nuke shut after power loss. PSEG Nuclear said its 1,150 megawatt Salem 1 nuclear power unit in Lower Alloways Creek, NJ was automatically shut on Tuesday, July 29, when its power supply was lost and the company declared an "unusual event."** An "unusual event" is the lowest of four emergency classifications set by the Nuclear Regulatory Commission to identify incidents at nuclear power stations. There was no threat to the health and safety of employees or the public, the company said in a statement, and the company does not know when the unit will be back in service. **PSEG Nuclear said it was investigating the cause of the power loss but said it appeared to be a breaker in the switchyard which developed an electrical fault.** All plant equipment and systems responded as expected, including three diesel generators that provided power to safely shut the unit.

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_07_29_eng-reuters_pma_PSEGS-N-J-SALEM-NUKE-SHUT-AFTER-POWER-LOSS&SMContentSet=0

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

3. *August 01, National Defense Magazine* — **Man-portable missiles imperil both military, civilian aircraft. Man-portable air-defense missiles, known as "manpads," are a continuing concern to military and civilian aviation operations. Manpads are shoulder-fired missile launchers that are effective up to 15,000 feet in altitude, and 3 miles in range.** Airplanes are safe at cruising altitude, but vulnerable shortly after takeoff and before landing. Although U.S. forces have had overwhelming control of the air space in Operations Enduring Freedom and Iraqi Freedom, they have not been able to curtail the proliferation of manpads, although the threat has diminished somewhat. The military is also concerned about manpads being used against civilian aircraft. The Bush administration set up a special panel to assess the vulnerability of U.S. airliners, and Congress has sponsored legislation, asking the Department of Homeland Security to address the problem and figure out how to best protect commercial aircraft.

Source: <http://nationaldefense.ndia.org/article.cfm?Id=1166>

4.

July 30, Dow Jones Business News — Navy selects team to design new combat ship. **The U.S. Navy has selected a team to finalize preliminary designs of a Littoral Combat Ship (LCS), the next-generation surface combatant.** The team has seven months to finalize designs, and upon successful completion of the preliminary design, the Navy will award contracts for construction of up to two LCS ships, with delivery of the first ship project as early as 2007. **The LCS will be a stealthy, high-speed ship capable of moving quickly in littoral or coastal areas at speeds at or above 50 knots.**

Source: http://biz.yahoo.com/djus/030730/0951001074_2.html

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

Banking and Finance Sector

Nothing to report.

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

Transportation Sector

5. *July 30, Portland Press Herald (Maine)* — **City wants U.S. to help guard port. Portland hopes to become the first seaport in the nation to have the federal Transportation Security Administration (TSA) take over passenger and baggage screening for maritime traffic.** Portland's Ports and Transportation Director Jeff Monroe has submitted a request to the TSA seeking a pilot program to make screeners from the Portland International Jetport responsible for security screening at the port. Portland officials hope the city's unusual position of having an international ferry terminal and cruise ship traffic will boost its chances of winning approval, Monroe said. **Federal screeners, either conducting the security checks or overseeing a private company, would standardize security with what is in place at airports. The lack of coordinated security in the nation's seaports is one of the reasons they are considered especially vulnerable to terrorist threats.** Passenger and baggage screening on Portland's waterfront is now done by private companies hired by the city or the shipping companies.
Source: <http://www.pressherald.com/news/local/030730security.shtml>

6. *July 30, Associated Press* — **U.S. may cut air marshals despite warning. The Transportation Security Administration (TSA) wants to reduce the number of air marshals to save money.** The TSA is seeking approval from Congress to cut \$104 million from the air marshal program to help offset a \$900 million budget shortfall. It's unclear how many of the estimated several thousand air marshal jobs would be affected. **"When we are faced with more priorities than we have funding to support, we have to go through a process of trying to address the most urgent needs,"** TSA spokesman Robert Johnson said. News of the air marshal program cutbacks come as the Department of Homeland Security is warning of the possibility of hijackings. A copy of the advisory, obtained Tuesday by The Associated Press, suggests an attack could take place by the end of the summer. The warning said terrorists may use five-man teams to take over airplanes just after takeoff or before landing and crash them into buildings.
Source: http://abcnews.go.com/wire/Politics/ap20030730_590.html

7. *July 30, The Day (CT)* — **Local railroad bridges in bad shape, says Amtrak chief. The president of Amtrak has singled out 90-year-old railroad bridges over the Thames and Niantic rivers as portions of the national rail system desperately in need of repair and “in danger of failing.”** Amtrak President David L. Gunn issued a written statement Monday in response to President Bush's proposal to dismantle Amtrak. Gunn urged federal lawmakers to approve next year's \$1.8 billion capitol budget request to fix the bridges and other looming problems even if Amtrak's long-term future is uncertain. **By “failing,” Gunn referred to mechanical malfunctions that could lock the movable bridges in the opened positions, crippling train travel along the Northeast Corridor. If either bridge failed, Gunn said, it would “stop service between New Haven and Boston until they are fixed or replaced.”** An Amtrak spokeswoman said Gunn did not mean to imply that the bridges are unsafe. “These bridges are not in danger of collapsing,” said Karina Van Veen, an Amtrak spokeswoman, who was unable to give the frequency of the bridge malfunctions or detail the exact structural problems.
Source: <http://www.theday.com/eng/web/newstand/re.aspx?reIDx=1EC70F88-3614-4715-8B85-81E8C405129>
8. *July 30, Associated Press* — **New Jersey transit nightmare after accident. Commuters and interstate travelers were delayed Wednesday morning as crews worked to restore power lines knocked down Tuesday evening by a passing train.** In the morning rush, most New Jersey Transit trains on the Northeast Corridor and North Jersey Coast lines were running 30 minutes to an hour behind. By 10 a.m., most delays were less than 30 minutes, said spokesman Ken Hitchner. Amtrak delays Wednesday were projected to be from two to five hours, Amtrak spokeswoman Karina Van Veen said. **Three of the four rail lines owned by Amtrak were closed south of Newark early Wednesday, causing significant delays as trains waited to pass on the one usable line. New Jersey Transit trains also use the lines.** The disruption comes on the heels of several major rail problems this month, including a train derailment, at least five incidents in which trains struck people on the tracks and a weather-related power outage. **The most recent trouble started at 6:25 p.m. Tuesday when an Amtrak Metroliner traveling from New York to Washington, DC, pulled down overhead power lines and stranded thousands of passengers for up to two hours. A passing Acela train's windshield was shattered, and authorities were investigating how that happened, Van Veen said.**
Source: <http://www.nynewsday.com/news/nyc-jerseytraffic.0.2296053.story?coll=nyc-topnews-short-navigation>
9. *July 30, Federal Computer Week* — **MBTA to get new communications.** Massachusetts Bay Transportation Authority (MBTA) will spend \$25.7 million to develop a new communications system. **The transportation authority, which operates the nation's oldest transportation system in the Boston metropolitan area, recently agreed to the contract for two-way, 800 MHz voice and data communications. Slated to go live by spring 2005, it will link MBTA supervisors, police, and bus and subway operators. They currently use different systems that are 10 to 20 years old,** said Mary Doherty, northeast area director with M/A-COM, a business unit of Tyco Electronics, based in Lowell, Mass. MBTA is just one of many transit systems around the country with communications systems that don't work together, Doherty said. **Interoperability has emerged as a primary need for governments across the country, although some states and regions have taken steps to improve their communications platforms through costly new digital systems or more inexpensive patches that connect**

existing networks.

Source: <http://www.few.com/geb/articles/2003/0728/web-mbta-07-30-03.asp>

10. *July 30, Government Accounting Office* — **GAO-03-843: Transportation Security: More Federal Coordination Needed to Help Address Security Challenges.** Published June 30 this report says the economic well being of the U.S. is dependent on the expeditious flow of people and goods through the transportation system. The attacks on September 11, 2001, illustrate the threats and vulnerabilities of the transportation system. **GAO was asked to examine the challenges in securing the transportation system and the federal role and actions in transportation security. GAO recommends that DHS and DOT use a mechanism, such as a memorandum of agreement, to clarify and delineate DOT's and TSA's roles and responsibilities in transportation security matters.** DHS and DOT generally agreed with the report's findings; however, they disagreed with the recommendation. Highlights:

<http://www.gao.gov/highlights/d03843high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-03-843>

11. *July 29, New York Times* — **Boeing tests effort to curb volatility in fuel tanks. Seven years after Trans World Airlines Flight 800 was destroyed by an explosion in its center fuel tank, Boeing is testing a 747 in which such explosions are nearly impossible, with a protective system that it is hoping to install on planes around the world. But in an era of airline bankruptcies, it is not clear who would pay, or how.** Even so, Boeing thinks the Federal Aviation Administration could certify the system's safety in the next few months. In a one-hour test flight today, a mostly empty Boeing 747-400 took off from Dulles International Airport and made a 300-mile loop around Virginia, as technicians in the main cabin read computer displays that measured the air in the tank. **Fuel tank explosions are unusual, but 737's exploded on the ground in Manila in 1991 and Bangkok in 2001.**

Source: <http://www.nytimes.com/2003/07/30/business/30PLAN.html>

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

Postal and Shipping Sector

12. *July 29, Bloomberg* — **Koizumi mulls postal service sale. Japanese Prime Minister Junichiro Koizumi may establish a committee of academics and other experts to consider a plan to sell off Japan's postal service operations.** Koizumi has described the sell-off of the three state-owned postal businesses, including mail, savings, and life insurance, as the centerpiece of his policy plan to be announced before Japan's Liberal Democratic Party's presidential election in September. Any plan to sell off the postal assets wouldn't likely become law until 2006 at the earliest and is expected to face strong objections from some of Japan's political groups.

Source: <http://quote.bloomberg.com/apps/news?pid=10000101&sid=a.GRurLk22fs&refer=japan>

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

Agriculture Sector

13. *July 30, Wisconsin Ag Connection* — **British propose emergency veterinary reserve. A new corps of private sector vets, able to join forces with the British Government at short notice to fight outbreaks of animal disease has been proposed.** Members of the group will be contracted to do five days paid training each year. In return, they will need to commit themselves to be available in an emergency. Initially, the Department of Environment Food and Rural Affairs will be looking to recruit around 100 vets to join this veterinary reserve. **In their training, the vets would be told their likely role in any outbreak, take part in exercises, and learn the management and organisational structures which would apply in times of emergency.**

Source: <http://www.wisconsinagconnection.com/story-national.cfm?Id=822&yr=2003>

14. *July 30, Associated Press* — **Plum pox found outside quarantine zone. The state has detected its first plum pox virus infection outside a quarantine zone in south-central Pennsylvania this season.** Two infected peach trees were found in Menallen Township, Adams County, west of a section of the township that had been previously quarantined, state Agriculture Secretary Dennis C. Wolff said Wednesday. Three growers who manage a 15-acre area where the trees were found have been notified, and all susceptible trees within 500 yards must be removed and destroyed, Wolff said. **The infected area will be added to the quarantine zone.** The virus has been discovered in four other peach trees and one ornamental flowering plant so far this year, according to the department.

Source: <http://pennlive.com/newsflash/pa/index.ssf?/base/news-5/1059593249165690.xml>

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

Food Sector

Nothing to report.

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

Water Sector

15. *July 30, Water Tech Online* — **EPA to fund new clean water research. The U.S. Environmental Protection Agency (EPA) has announced it will provide over \$10 million in research grants, some of which will be spent on studying the long-term health effects of watershed protection.** EPA Assistant Administrator for Research and Development Paul Gilman said that the funding is part of the EPA's commitment to base policy decisions on the highest quality science. These research grants were awarded through EPA's Science to Achieve Results (STAR), which funds scientific work through competitive application and independent peer review processes. The watershed protection projects were also funded through an agreement with the US Department of Agriculture.

Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=42002

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

Public Health Sector

16. *July 30, Daily Texan* — **Smallpox drill. As part of an emergency preparedness drill Tuesday, 120 mock patients checked themselves into hospitals around Austin, TX reporting symptoms of smallpox.** The University of Texas (UT), the city of Austin Health and Human Services Department, and 10 Austin hospitals contributed to a drill where patients feigned the disease to test responses of emergency staff. Lindy McGinnis, with the city of Austin Emergency Management Office, said the test had two phases. The volunteers checking into hospitals was Phase I. **"We have several volunteers checking into the hospital with symptoms of smallpox," McGinnis said. "We're testing emergency units' ability to identify the symptoms, do all the right tests, and deal with all the issues."** Phase II had volunteers getting mock vaccinations in three sites in Austin to simulate the U.S. Center for Disease Control's response to an outbreak. Beth Bushey, vaccination clinic coordinator for UT said that 24 sites in Austin would undertake the task of vaccinating 1.4 million people in the case of an actual outbreak. Phase II tested how selected vaccination sites handled that many people. "We're taking 50 people and seeing how long it takes to vaccinate them, then extrapolating that out to a large number of people," she said.
Source: <http://www.dailytexanonline.com/vnews/display.v/ART/2003/07/30/3f277d0a4b52d>

17. *July 30, Nature* — **Artificially evolved protein destroys nerve gas.** Chemists have modified a common bacterial enzyme so that it pulls apart a lethal nerve agent manufactured as a chemical weapon. **Frank Raushel, of Texas A&M University, and colleagues tuned the enzyme phosphotriesterase to destroy the nerve gas soman. A more efficient version could form part of a mask to protect against nerve agents, Raushel suggests.** Phosphotriesterase naturally breaks down soman, but slowly. **Raushel's team has increased its activity by a factor of 1,000. This is still not fast enough to be useful, but the researchers anticipate that further tweaks should make the enzyme work even better.** In bacteria, phosphotriesterase severs chemical bonds between phosphorus and oxygen atoms. It has been investigated before for cleaning up pollution from toxic organophosphorus pesticides and herbicides.
Source: <http://www.nature.com/nsu/030728/030728-7.html>

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

Government Sector

18. *July 30, Government Computer News* — **Homeland Security extends smart-card deal for 10 years. The Homeland Security Department has awarded a 10-year, \$200 million follow-on contract to an existing five-year identification card deal.** Datatrac Information Services Inc. will continue to provide services to the department under the Integrated Card Production System contract. **The Richardson, Texas, company has produced several million permanent resident cards, border crossing cards and employment authorization documents for the Bureau of Citizenship and Immigration Services (BCIS), the former Immigration and Naturalization Service.** The contract's base period is one year, with nine option years, said Dennis M. Priscandaro, program manager for Datatrac. Through the project, the trio of companies will create smart cards that can hold identity information, including biometric data, according to the company.
Source: http://gcn.com/vol1_no1/daily-updates/22942-1.html

19. *July 29, New York Times* — **Model–rocket bill stirs debate.** At a time when Congress has been seeking to strip terrorists of potential tools, some lawmakers are pushing legislation that opponents say would do just the opposite by easing restrictions on explosives used in model rockets. **Legislation pending in the Senate would exempt some model–rocket propellants from toughened restrictions on explosives that were imposed by Congress last year in response to the terrorist attacks of September 11, 2001.** The proposed exemption grew out of complaints from rocket hobbyists who said the new regulations would essentially ground them by requiring many users of model rockets to register with the federal government and go through background checks before using certain regulated explosives to launch their rockets. But the effort to lift those restrictions is now drawing sharp objections from several lawmakers **and from the Justice Department, which warned that one version of the legislation would give terrorists the power to hit targets five miles away.** Regulations imposed by Congress last year in the Safe Explosives Act restricted several chemicals used in high–power rocketry, including a propellant known as APCP and a compound known as black powder.
Source: <http://www.nytimes.com/2003/07/30/national/30ROCK.html>

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

Emergency Services Sector

20. *July 30, Clarksdale Press Register (MS)* — **County officials defend emergency plan.** Supporters of the plan to ditch the county's outdated warning sirens in place of an emergency telephone notification system defended the move this week. **Coahoma County (Mississippi) District 2 Supervisor Chris Overton and Emergency Management Director Johnny Tarzi said using the new system would alert more people to danger than would the county's seven warning sirens. Provided by Colorado–based Intrado Inc., the telephone notification system would send a recorded message to thousands of telephone numbers in a short period of time.** But the plan has its critics. Former Clarksdale resident Kristin Barber said that the new system overlooked a large portion of the local residents – namely, those without telephones. According to the U.S. Census Bureau 2000 census report, 8.8 percent of Coahoma County households do not have telephones. **Overton said that even if the new system doesn't reach the few people without telephones, it will still reach more people than the warning sirens did. None of the county's seven sirens were located outside the city limits,** Tarzi said, and three of those sirens have been inoperable for more than a year.
Source: http://www.zwire.com/site/news.cfm?newsid=9926029&BRD=2038&PAG=461&dept_id=230617&rft=6

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

Information and Telecommunications Sector

21. *July 31, Herald Sun (Australia)* — **Report reveals vulnerabilities in Australian infrastructures. An official report on an Australian government website reveals how vulnerable the country is to attack.** Written by a former government security analyst, it was prepared in the lead–up to the 2000 Sydney Olympics. **"Computers cannot operate without power," the report says. "Nor can telecommunications, the financial network or defense**

communications." The report reveals the locations of Melbourne's gas supply and the weakest link in the oil and gas pipeline; the location of the central computer to shut down the electricity for New South Wales; the electricity sub stations supplying power to the national capital; the critical telephone exchanges to attack to sever communications between eastern and Western Australia and from the rest of the world; casts doubt on to the Reserve Bank's claims that its computer systems are secure; and details how to disrupt radio and TV communication to the public in the event of an attack. Matt Warren, director of the Australasian Institute of Network Information Warfare, said **if terrorists successfully attacked simultaneously all the weak spots identified in the report, the result would be an unprecedented disaster.**

Source: <http://www.ds-osac.org/VIEW.CFM?KEY=7E445D4B4556&TYPE=2B170C1E0A3A0F162820>

22. *July 31, U.S. Department of Homeland Security* — **The Department of Homeland Security updated "Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems".** The Department of Homeland Security (DHS)/Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCS) is issuing this updated advisory in consultation with the Microsoft to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting a Remote Procedure Call (RPC) vulnerability in some Microsoft Windows operating systems. **Several working exploits now in widespread distribution on the Internet provide full remote system level access to vulnerable computers. No worm code has been reported,** but an Internet-wide increase in scanning for vulnerable computers over the past several days reinforces the urgency for updating affected systems. Microsoft updates and workarounds are available at <http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>. **DHS and Microsoft further suggest that Internet Service Providers and network administrators consider blocking TCP and UDP ports 135, 139, and 445** for inbound connections unless absolutely needed for business or operational purposes.

Source: http://www.nipc.gov/warnings/advisories/2003/Potential730200_3.htm

23. *July 30, Government Computer News* — **Security group issues compromise plan for vulnerability reporting.** The Organization for Internet Safety (OIS) has released a guide for reporting and responding to software security vulnerabilities. **The voluntary guidelines are an effort to balance the public's right to know about possible problems against the need for vendors to correct those problems before they are made public.** They call for: cooperation between the discoverer of a flaw and the software vendor; a waiting period, typically 30 days, to let a vendor to correct a problem before it is publicly announced; a 30-day grace period to let users to fix their systems before technical details that could help attackers are released. Over the past several years a consensus has developed that makers should be given a chance to fix problems before they are exposed. **Hackers, however, assert that the only way to ensure that software makers fix problems is to publicly expose them.** The guidelines are available on the OIS Website: www.oisafety.org

Source: http://www.gcn.com/vol1_no1/daily-updates/22952-1.html

24. *July 28, IDG News Service* — **Standards bodies meet to coordinate efforts.** Leaders of 36 IT standards bodies and industry consortia met last week in San Francisco, CA, at the Informal Forum Summit of the International Telecommunication Union's Telecommunication

Standardization Sector (ITU-T), where they shared insights and discussed possible areas of cooperation. Most of the discussion revolved around ways to facilitate communication in the future rather than actual cooperative initiatives between specific bodies, Houlin Zhao, director of the ITU's Telecommunication Standardization Bureau (TSB), said. **A broad statement agreed on by the 69 representatives at last week's meeting called for cooperation to increase the collective value of the technologies they work on and allow for a more accessible global information network, Zhao said. It also called for cooperation to accelerate standardization of technologies, share best practices, leverage economies of scale and improve interoperability.**

Source: http://www.infoworld.com/article/03/07/28/HNstandardsbody_1.html

25. July 28, Wired — Draft of telecommunications bill of rights released. California State Public Utilities Commissioner (PUC) Carl Wood said his team has drafted the final version of a Telecommunications Consumer Bill of Rights, which could become law in September. **The proposed law would require all phone companies, including wireless, local and long distance, to be upfront about the quality of their services and provide the utmost customer care.** Among other provisions, companies would have to disclose key rates, contract terms and conditions, and prices clearly on all print material, advertising and websites. In addition, **customers would be given 45 days to cancel their contracts without penalty if they are not satisfied with their service.** The PUC originally drafted the bill in response to the volume of complaints it received from customers regarding their phone companies. Two years ago, 31,345 California residents filed grievances with the state. The draft is available here:

<http://www.cpuc.ca.gov/static/Industry/Telco/030723borwooddr aftdec.doc>

Source: <http://www.wired.com/news/business/0,1367,59789,00.html>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_LOVGATE.F Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios-ns), 80 (www), 445 (microsoft-ds), 1434 (ms-sql-m), 139 (netbios-ssn), 4662 (eDonkey2000), 113 (ident), 0 (----), 25 (smtp), 19479 (----) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

26. *July 30, Reuters* — **U.S. says terrorists may be using east Africa. U.S. Central Command chief General John Abizaid said Wednesday, July 30, that east Africa could still be a transit and operational zone for terrorists, and urged states in the region to combat the threat. Abizaid was in Addis Ababa for a meeting of 11 east African countries at which they agreed to set up a U.S.–backed system for preventing and dealing with terror attacks and other disasters. The region is seen as highly susceptible to terrorist groups, who take advantage of porous borders and a lack of tight central control.** The 11 countries at the meeting were Burundi, the Democratic Republic of Congo, Djibouti, Egypt, Eritrea, Ethiopia, Kenya, Rwanda, Seychelles, Tanzania and Uganda. The two–day "Golden Spear" symposium, an annual meeting to discuss disaster prevention, was attended by ministers and senior military representatives.

Source: <http://reuters.com/newsArticle.jhtml?type=worldNews&storyID= 3189516>

27. *July 30, The Arizona Republic* — **14 arrested in alleged money–laundering operation. A joint terrorism task force based in Phoenix, AZ, arrested 14 people across the East Valley on Wednesday, July 30, on charges of running a money–laundering operation that brought in \$11 million through the sale of stolen infant formula.** The 14 people arrested in the Valley are accused of money laundering, interstate transportation of stolen property and making false statements in dealings with food–stamp programs. Authorities allege that Samih Jamal of Mesa, AZ, employed others to steal or fraudulently obtain infant formula around the country and transport it to Phoenix and other locations where the formula was repackaged and shipped to wholesalers across the country. **The Valley crackdown was almost identical to a series of raids in Dallas last month that led to the arrests of 11 people who were accused of running an infant formula theft ring that funneled millions of dollars in profits to several Middle Eastern countries.**

Source: <http://www.azcentral.com/news/articles/0730terrorraid30–ON.h tml>

28. *July 30, Associated Press* — **Forecasts of rising winds have fire officials worried. Forecasts of rising winds and temperatures near 100 degrees on Wednesday signaled another hard day coming for the 900 firefighters trying to keep a wildfire away from Glacier National Park’s west entrance.** The Robert Fire advanced some 2,000 acres Tuesday, to 14,200 acres, park officials said Wednesday morning. West Glacier, on the west–central edge of Glacier National Park, was mostly empty, save for emergency workers and about 60 residents who ignored Monday’s order to leave. About 500 residents evacuated from Glacier and the surrounding area Monday night after authorities grew concerned a main escape route would be cut off. **Amtrak said its Empire Builder passenger train was no longer stopping in West Glacier, and was diverting passengers to Whitefish or Essex.**

Source: <http://www.billingsgazette.com/index.php?tl=1&display=rednews/2003/07/30/build/local/15–fireweather.inc>

[[Return to top](#)]

DHS/IAIP Products & Contact Information

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

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

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

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

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-6631

Subscription and Distribution Information: Send mail to 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 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.