



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 28 July 2003

Current Nationwide Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports a Russian computer hacker was sentenced to four years in federal prison for running a fraud and extortion ring that victimized among others a New Jersey financial services company. (See item [5](#))
- The Journal News reports a toxic chlorine gas leak, discovered Thursday morning at a plant that treats New York City's drinking water, led officials to evacuate about 75 workers and hundreds of children attending two nearby summer camps. (See item [10](#))
- The Philadelphia Inquirer reports that when the blackout hit on July 7, Glenmede Trust Co. experienced an unplanned test of the disaster recovery plan it had designed after 9/11, a test of its technical systems as well as employee discipline. (See item [20](#))
- Internet Security Systems has raised AlertCon to Level 3, due to at least one functional exploit code in connection with the RPC vulnerabilities. Please refer to the Internet Alert Dashboard.

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 25, The Associated Press* — Shipped uranium to make fuel in Tennessee. The first shipments of some 33 metric tons of former weapons-grade uranium have been moved

from the Savannah River Site in South Carolina to Tennessee, where the Tennessee Valley Authority (TVA) has agreed to accept the uranium after it has been diluted for use in commercial reactors. According to Secretary of the Energy Spencer Abraham, "we have taken material that was left over from the Cold War and turned it into something that is unattractive for use in weapons. Not only that, but we've turned it into a material that has an important peacetime use, producing energy." TVA operates three nuclear facilities; Watts Bar and Sequoyah in Tennessee, and Browns Ferry in Alabama. The shipments, which began two weeks ago, are expected to continue through 2007.

Source: <http://www.nytimes.com/aponline/national/AP-BRF-Uranium-Shipments.html>

- 2. July 25, Nuclear Regulatory Commission — NRC finds Indian Point meets reasonable assurance criteria for emergency preparedness. The Nuclear Regulatory Commission (NRC) has determined, from its continuing evaluation of the licensee's on-site emergency planning and preparedness for radiological events, that Indian Point nuclear facility in Buchanan, NY, meets the requisite criteria for reasonable assurance of adequate protection.** The Federal Emergency Management Agency (FEMA) has responsibility for assessing off-site emergency preparedness, including the coordination and implementation of radiological protection guidelines. NRC has responsibility for assessing on-site emergency planning and preparedness; the specific requirements and oversight are established for NRC licensees to ensure adequate protection of public health and safety. Considering both FEMA's off-site and NRC's on-site emergency preparedness assessments, the NRC's overall determination continues to be that Indian Point emergency preparedness is satisfactory and provides reasonable assurance of adequate protection.

Source: <http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-099.html>

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

- 3. July 25, The Associated Press — Boeing barred from future rocket work. The Air Force ruled that Boeing Co. broke the law by stealing rival Lockheed Martin Co.'s trade secrets and, as a penalty, took away seven military satellite launches that were to use Boeing rockets and indefinitely banned Boeing from bidding on future satellite-launching contracts. Further punishment includes allowing Lockheed Martin to build a \$200 million launch pad at Vandenberg Air Force Base in California to compete with Boeing for West Coast launches. Air Force Undersecretary Peter Teets said an Air Force investigation concluded that Boeing committed "serious and substantial violations of federal law" by stealing extensive information from Lockheed Martin during competition for a \$1.88 billion satellite launching contract in 1998.**

Source: http://customwire.ap.org/dynamic/stories/B/BOEING_CONTRACT?SITE=DCTMS&SECTION=HOME

4. *July 24, CNN* — **Charges over China weapons exports. Two California-based men have been charged with trying to export military components for fighter jets, helicopters and surface-to-air missiles to China.** According to the Bureau of Immigration and Customs Enforcement (ICE), "for investigative purposes, undercover ICE agents posed as representatives of a fictitious Chinese company called Sino-American Aviation Supply. Purportedly based in Shenyang, China, [the company] sought to purchase U.S. defense articles for shipment to and use in the People's Republic of China." **Beginning in November 2000, and continuing through June 2001, the indictment alleges, the defendants acquired several controlled military components for F-4 and F-5 fighter jets, which they then attempted to export to China without fulfilling State Department requirements.**

Source: <http://www.cnn.com/2003/US/07/24/china.exports/index.html>

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

Banking and Finance Sector

5. *July 25, Associated Press* — **Russian computer hacker gets four year term. A Russian computer hacker was sentenced to four years in federal prison for running a fraud and extortion ring that victimized a New Jersey financial services company, among others.** An indictment accused the hacker and his accomplices of hacking into dozens of U.S. banks and e-commerce sites, and then demanding money for not publicizing the break-ins. It was determined that the ring leader, Aleksey Ivanov, cost victims about \$25 million. **The New Jersey fraud involved Ivanov hacking into the computer system of Financial Services Inc. (FSI) of Glen Rock, a Web hosting and electronic banking processing company on March 22, 2000. He stole 11 passwords that FSI employees used and a file with about 3,500 credit card numbers.** An unnamed cohort then threatened that the hackers would release the credit card numbers and damage the FSI computer system unless FSI paid \$6,000. After negotiations, FSI wired \$5,000 in April and May 2000 to a Moscow bank. That November, the FBI tricked Ivanov and an accomplice into traveling to Seattle by posing as potential customers from a mock company called Invita Computer Security. Undercover agents asked the pair for a hacking demonstration, then arrested them.

Source: http://www.boston.com/dailynews/206/region/Russian_computer_hacker_gets_4:.shtml

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

Transportation Sector

6. *July 25, CNN* — **Teen's Eagle Scout project used by airport security.** Travelers at the world's busiest airport are waiting less at security checkpoints thanks to the tinkering of a 15-year-old Boy Scout. **Josh Pfluger and his scouting pals went into his Rockford, IL, garage and hammered out a shoe-scanning device now in daily use at O'Hare International Airport. His goal at the time was simply to polish off his Eagle Scout requirements.** Pfluger's homemade invention -- **a box with a metal detector that travelers step onto before they reach the security gate** -- is an optional, preliminary step to let

passengers know whether their shoes will trigger alarms at the gate. **That can speed up lines by tipping passengers off they may need to remove their shoes and send them through X-ray machines — and maybe even encourage people to leave footwear with metal eyelets behind on future trips.** With help from his dad, Dan Pfluger, Josh and about 10 others put in a total of 120 hours to design and build more than a dozen scanners, which feature sliding boards with Plexiglas. **Inside each box is a wand, or small metal detector, held up with bungee cords; the box sounds an alarm if there's a violation. With Josh's inspiration, each one has a flag, the TSA logo and "Place foot here" on the top.** The invention has earned Pfluger lots of attention — and a possible career.

Source: <http://www.cnn.com/2003/TRAVEL/07/25/scout.shoe.scanner.ap/index.html>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

7. *July 25, Katu.com* — **Fungus threatens Oregon's hazelnut industry. Agriculture officials are asking Willamette Valley, OR farmers to chop down some filbert trees in an emergency attempt to prevent the spread of a virulent fungus that threatens the state's \$23 million hazelnut industry.** Farmers must destroy up to six acres of filberts at two orchards south of Coburg, or about 650 trees said Ross Penhallegon, an Oregon State University horticulturist. Growers and state officials have been trying for years to prevent the blight's spread southward. **The disease was detected in 1999 in Keizer, north of Salem, OR. Previously, it had wiped out the filbert industry in Washington, Penhallegon said. In the United States, only Oregon produces hazelnuts.** The state's output is 3 percent to 4 percent of world production. Officials want broader, radical measures in the face of the extensive new discoveries, Penhallegon said. These may include having growers at the end of the current season cut down and dispose of specialized types of filbert trees that are particularly susceptible to the disease, even though they do not show signs of it, he said. Growers will have to plant disease-resistant varieties, he said. They'll also need to spray fungicides up to three times a year, he said.

Source: <http://www.katu.com/business/story.asp?ID=59400>

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

Food Sector

8. *July 25, Exponent* — **Researcher aims to eradicate deadly bacteria. Inside an uncooked hot dog or refrigerated lunchmeat could be deadly bacteria with a fatality rate of 20 percent; a Purdue University researcher is hoping to find a way to reduce that number.** *Listeria monocytogenes* can be found almost everywhere. If food is not packaged and handled properly, *Listeria* can contaminate it and people may become ill with listeriosis. **Arun Bhunia, associate**

professor of molecular food biology, is researching how the bacteria enter the intestines. He hopes his work will help in the formulation of a medicine that would be able to block Listeria from entering the intestinal cell wall. He and his co-researcher are the first to do a comprehensive study where numerous strains of Listeria were tested for all three aspects of infection; adhesion, invasion, and translocation, said Bhunia. **"If we could block the binding of the bacteria to cells then the bacteria could no longer cause disease," he said.** When people eat the contaminated food, the first place it binds is the intestinal tract. The bacteria could then spread and cause liver and spleen damage as well as encephalitis and meningitis. It could also cause pregnant women to have miscarriages.

Source: <http://www.purdueexponent.org/interface/bebop/showstory.php?date=2003/07/25§ion=campus&storyid=listeriainfectionprocess>

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

Water Sector

9. *July 25, Water Tech Online* — **\$1.7 million awarded for water terrorism safety assessment. As part of the U.S. Environmental Protection Agency's (EPA's) continuing efforts to help drinking water utilities assess their vulnerabilities to terrorist attacks, EPA's Office of Water has awarded two grants totaling \$1.7 million to the International City/County Management Association (ICMA) and the Water Environment Federation (WEF).** Through a combination of training sessions, on-site technical assistance, and Internet-based tools, the ICMA and WEF will target training to the approximately 480 community water systems that serve 50,000 to 100,000 people, the release said. Community water systems of this size are required to submit a vulnerability assessment to EPA on or before Dec. 31. They must also certify completion of an emergency response plan six months after submission of a vulnerability assessment.

Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=41928

10. *July 25, Journal News (New York)* — **Chlorine leak at water plant prompts evacuation. A toxic chlorine gas leak discovered Thursday morning at a plant that treats New York City's drinking water led officials to evacuate about 75 workers and hundreds of children attending two nearby summer camps.** No one was injured. The leak was contained in the Shaft 18 building at the New York City Department of Environmental Protection's (DEP) Valhalla campus. The facility treats the city's and most of Westchester's drinking water from the Catskill and Delaware reservoir systems. **The city's water system was not affected, said Ed Welch, chief of the DEP Police.** Members of the DEP Police hazardous materials team entered the building after an alarm was triggered shortly before 9 a.m., Welch said. Chlorine levels reached 28 parts per million, almost three times the amount that would trigger the alarm, he said. Chlorine is a hazardous gas that can irritate the eyes and respiratory tract and cause coughing, teary eyes, choking and chest pains. In sufficient quantity, exposure can be fatal. **The leak likely started when the valves were replaced Wednesday night as part of a regular maintenance program, Welch said.**

Source: <http://www.nyjournalnews.com/newsroom/072503/a0125kensico.html>

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

Public Health Sector

11. *July 25, CNN* — **New Hong Kong SARS outbreak ruled out. Eighteen people suspected of having the Severe Acute Respiratory Syndrome (SARS) virus at a Hong Kong psychiatric institution are in fact suffering from influenza, the territory's government has announced.** In a statement Friday, officials said tests had "yielded positive results for Influenza A" while none had come up positive for SARS. News of the suspect SARS cases had raised fears that the virus had made a comeback in Hong Kong about a month after the territory was declared SARS-free. The patients, all residents at a mental health institute, had been suffering from "respiratory problems such as fever and coughs," a government spokeswoman said.
Source: <http://www.cnn.com/2003/WORLD/asiapcf/east/07/25/virus.hk/>

12. *July 25, Tucson Citizen* — **Bill seeks funds for border health security. A group of border-state lawmakers, led by Arizonan Senator John McCain and Representative Jim Kolbe, wants Congress to pump \$235 million into the region to improve health services for millions of residents and prepare communities for a potential bioterrorism attack.** House and Senate lawmakers this week introduced a bill in both chambers that would provide \$200 million in grants for scores of health-related projects by local and state governments, colleges and universities, tribal governments and nonprofit health organizations. **The bill also would set aside \$25 million to build a health alert network, allowing health providers to communicate with each other easily during an outbreak of smallpox, anthrax, or other bioterrorism threat.** The remaining \$10 million would go to the U.S.–Mexico Border Health Commission in El Paso, Texas. Lawmakers argue that the bioterrorism dollars are sorely needed because border security is critical to national security. "As our nation enters a new era of heightened national alert, it is incumbent upon us to ensure our border area, our front line of defense, is strengthened and protected," McCain said.
Source: http://www.tucsoncitizen.com/local/7_25_03border_bill.html

13. *July 25, Associated Press* — **Fort Detrick tests new anthrax vaccine. Work done at the Army's research institute at Fort Detrick, MD has led to clinical trials across the country for a possible new anthrax vaccine. The new vaccine would require only a few injections, compared with the six shots required with the existing vaccine, researchers said.** At Fort Detrick, the research team singled out the protein in *Bacillus anthracis*, the bacterium that causes anthrax, that induces antibodies that neutralize anthrax toxins. The team then produced the protein, which is called "protective antigen," in a form that was free of other components of the bacteria. Researchers turned the bacteria against itself, using a crippled form of *Bacillus anthracis* to produce the necessary protein to create the vaccine. The result was called recombinant protective antigen, or "rPA," a purified protein designed to induce antibodies that neutralize anthrax toxins. **At the University of Maryland, a trial testing the original formulation of rPA has begun. A biopharmaceutical company in California has also begun clinical trials with about 100 volunteers at four medical centers.** "The advantage of the new technology is you you can get millions of doses at a relatively good price," said Ed Nuzum, of the National Institute of Allergy and Infectious Diseases.
Source: http://www.washingtonpost.com/wp-dyn/articles/A45923-2003Jul_25.html

14. *July 24, Federal Computer Week* — **Smallpox systems incomplete. The system used to report and track smallpox vaccines is incomplete and not fully electronic, Julie**

Gerberding, director of the Centers for Disease Control and Prevention (CDC), told lawmakers Thursday. Concerns about compensation and liability, as well as recipients having adverse reactions to the vaccine, have slowed the smallpox program, she said. **However, a system used to monitor adverse reactions has proven successful. "We have the best monitoring system we've had for any vaccine," Gerberding said.** The agency has made strides in an effort to better prepare the public health community for a bioterrorism attack, she said. Expanded health alert networks and laboratory response networks are aiding communications in the public health community. The Laboratory Response Network links 117 labs across the country so they can work together to combat bioterrorism and natural outbreaks of diseases. Fifty of those labs can detect and analyze Biosafety Level (BSL)-3 highly pathogenic organisms, which is triple the number of labs able to do so in 1999. Much work remains, Gerberding said. CDC is "starting with a public health system that's been long neglected," she told lawmakers at today's hearing.

Source: <http://www.few.com/few/articles/2003/0721/web-bio-07-24-03.a.sp>

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

Government Sector

15. *July 25, Government Executive Magazine* — **Arizona GOP introduces border security bill.** Sen. John McCain, (R-AZ), along with fellow Arizona Republican Reps. Jim Kolbe and Jeff Flake Friday **introduced the "Border Security and Immigration Improvement Act."** **Under their bill, individuals who entered the country illegally by August 1 could pay a fine and then be issued a three-year temporary work visa, with an option to reapply at the end of that time.** A second group of immigrants—those still seeking to enter the country—would be issued a renewable three-year temporary worker visa. Employers seeking to find foreign workers would be able to post the jobs electronically, but only after 14 days where the job would be made available to U.S. citizens. **The legislation hopes to address the United States' growing labor demand, as well as allow federal agencies to concentrate their efforts on terrorism and national security rather than on catching immigrants at the border.**
Source: <http://www.govexec.com/dailyfed/0703/072503cd2.htm>

16. *July 25, Government Executive Magazine* — **Homeland Security may retain standard pay system. Employees at the Homeland Security Department may end up with a pay structure that looks much like the one they have: the General Schedule (GS) system.** That's just one possibility that has evolved from a months-long process in which employees have played a significant role in designing HSD's new personnel management structure. On Friday, the design team responsible for developing personnel reform options for the civil service system at the Homeland Security Department presented their findings to a review committee of management and union officials. One of the options included shifting all HSD employees to the General Schedule system. According to team members, **the benefits of retaining the General Schedule included avoiding disruption caused by switching to a new system, the General Schedule existing classification system, its built-in appeal rights and its performance-based features.**
Source: <http://www.govexec.com/dailyfed/0703/072503t1.htm>

17.

July 25, Federal Computer Week — **Senate passes Homeland funding. On July 24, the Senate passed a \$29.3 billion appropriations bill for the Homeland Security Department (DHS) that adds new money for a variety of high-tech systems and orders reports on others before they are implemented.** House and Senate negotiators will try to reconcile differences between the Senate and House versions of the first DHS appropriations bill after lawmakers take an August vacation. The spending bill was approved 93-1, with Sen. Ernest Hollings (D-SC), casting the lone dissent because he wanted more money for port security. The major difference in the bills is that the Senate version provides no money for President Bush's Project BioShield, an \$890 million program to develop new technologies to combat biological warfare. **Lawmakers also approved a plan to review DHS' color-coded nationwide terrorist alert system that has come under fire because it is so costly to local communities each time the alert system is elevated. And they ordered a report on the vulnerabilities of large sports and entertainment facilities.**

Source: <http://www.few.com/few/articles/2003/0721/web-dhs-07-25-03.a.sp>

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

Emergency Services Sector

18. *July 25, Chicago Sun Times* — Chicago aldermen decide it's time to increase security.

Skittish aldermen Thursday called for stepped up security at Chicago's City Hall—including metal detectors in the lobby—but Mayor Daley said he sees no need to "lock down" the seat of city government. "This is City Hall. If you want to lock it down—if you don't want to let the people in, you won't let the people in," Daley said. **The New York shooting, on Wednesday, sent shock waves through Chicago's City Hall, primarily because Chicago's seat of government is nowhere near as secure as New York's.** In New York, people go through screening in a plaza outside City Hall and pass through metal detectors before entering the building itself. In Chicago, metal detectors are brought in only to screen people attending City Council meetings. **Chicago's City Hall is also attached to the Cook County building, and people move freely from one side to the other. There are four public entrances.**

Source: <http://www.suntimes.com/output/news/cst-nws-secr25.html>

19. *July 25, The Clarion-Ledger* — Mississippi cities react to New York shooting. Some city councils around the state are rethinking security measures following the shooting of a New York City councilman on Wednesday. Jackson and Meridian are among Mississippi cities planning to boost security measures in the near future. "Some changes have to be made," said Jackson City Council President Marshand Crisler. "We'll restrict the access to the City Hall." One guard and two Jackson Police Department officers protect Jackson council members during every meeting, said Thomas Kaelin, security guard supervisor at Mayor Harvey Johnson's office. **Jackson council members do not have to go through metal detectors while entering the temporary City Hall, said Ward 2 Councilman Leslie McLemore. All the visitors should go through the metal detectors, but they often violate this procedure, he said.** "The security procedures were not strictly enforced here," said McLemore, who put revision of security policy on Monday's work session agenda. "We saw that we shouldn't take anything for granted." **Meridian Mayor John Robert Smith said council members and visitors previously have not had to go through metal detectors inside City Hall. "Now, every one will have to go through detectors," Smith said.**

Source: <http://www.clarionledger.com/news/0307/25/m02.html>

20. *July 25, The Philadelphia Inquirer* — **Blackout tests Philadelphia company's disaster–recovery plan.** When the lights went out at One Liberty Place on July 7, Glenmede Trust Co. — like others in the building — experienced a nerve–wracking test of the disaster recovery plan it had beefed up after 9/11. **The blackout tested not only Glenmede's technical systems, but also employee discipline and management's ability to make the quick decisions to spend money that declaring a disaster requires.** Their planning allowed the company to continue to keep clients abreast of activity on Wall Street, place securities trade orders and handle wire transfers of funds. **Increasingly customers and vendors want to know that the companies they deal with are prepared to continue operating in emergencies, said Bob Dilossi, a disaster recovery specialist with SunGard Availability Services, based in Wayne.** On July 7, due to problems at Peco Energy Co., both power lines serving One Liberty Place, the city's tallest building, went dark. Glenmede — along with all other tenants in the 61–story building — were evacuated, triggering the first real test of many disaster plans. **The company's emergency preparedness plan already is being fine–tuned. The next time there is a crisis, for example, the Web site that serves the public will continue to function.**

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_krt.htm?SMDOCID=knightridder_2003_07_25_krtbn_0000-0098-PH-BLACKOUT&SMContentSet=0

[[Return to top](#)]

Information and Telecommunications Sector

21. *July 25, Federal Computer Week* — **New guidance for incident reporting.** The Bush administration will soon give agencies specific directions on how to report information security problems to the Federal Computer Incident Response Center (FedCIRC), said Sallie McDonald, a senior official within the Homeland Security Department's Information Analysis and Infrastructure Protection directorate. **The guidance, due within six weeks, will ensure that FedCirc is receiving the information it needs to best track, analyze and, if possible, prevent incidents that occur across agencies,** she said during a panel on Friday, July 25 at the GovSec 2003 conference in Washington, DC. The department's National Cyber Security Division houses FedCIRC and other national and governmentwide warnings and analysis groups that were spread around government. **State governments are also concerned about having a centralized view of security information,** said Chris Dixon, issues coordinator for The National Association of State Chief Information Officers. NASCIO is still working on technology and policies for its Interstate Information Sharing and Analysis Center, which will collect data from states across the country.

Source: <http://www.fcw.com/fcw/articles/2003/0721/web-security-07-25-03.asp>

22. *July 25, Government Computer News* — **Cyberthreats dog old DoD systems, House panel hears. The Department of Defense's (DoD) growing reliance on information networks for everything from conducting business to launching missiles makes cyberterror a big concern,** congressional and DoD officials said last week. "While programmers and software developers build more advanced systems to run more tasks, criminals become more creative in their methods to break into these systems," said Rep. Jim Saxton (R–NJ), chairman of the

House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities. Robert Lentz, DoD's director of information assurance, "The growing sophistication of attack makes speed of attack and response absolutely critical." The department's three million computers, 100,000 LANs and 100 long-distance networks are all part of the Global Information Grid. **Last year, the department successfully blocked about 50,000 attempts to gain root-level access to systems, he said. One problem with security stems from antiquated IT equipment, Lentz said, because information assurance goes hand in hand with modernized networks.**

Source: http://www.gcn.com/vol1_no1/daily-updates/22897-1.html

Internet Alert Dashboard

Current Alert Levels	
<p>AlertCon: 3 out of 4 https://gtoc.iss.net</p>	<p>Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/</p>
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_LOVGATE.G 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	80 (www), 445 (microsoft-ds), 137 (netbios-ns), 1434 (ms-sql-m), 139 (netbios-ssn), 4662 (eDonkey2000), 113 (ident), 0 (----), 53 (domain), 25 (smtp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

23. July 26, Washington Post — Shelling hits U.S. embassy in Liberia. President Bush directed the Pentagon to position U.S. Marines off the coast of Liberia Friday, July 25, to assist the arrival of West African peacekeepers, as fighting intensified between government and rebel forces. U.S. defense officials said a three-ship Amphibious Ready Group with 2,200 Marines led by the helicopter carrier USS Iwo Jima would arrive in the region from the Mediterranean in early August, about the time Nigeria has pledged to dispatch the first battalion of Nigerian peacekeepers into Liberia. The president made his announcement as Monrovia, the Liberian capital, witnessed its worst violence in days as rebel forces bent on ousting President Charles Taylor pressed their offensive. Shells crashed into the U.S. Embassy grounds Friday, and a daybreak mortar attack on a school packed with refugees Saturday killed at least 26 people and wounded more than 200, the Associated Press reported.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A48403-2003Jul 25.html>

24. *July 26, Reuters* — **Quakes jolt northeastern Japan, hundreds hurt. A series of strong earthquakes hit northeastern Japan on Saturday, July 26, injuring more than 420 people and causing some 2,500 people to evacuate**, officials and media said. The earthquakes were centered in Miyagi prefecture, about 190 miles north of Tokyo. The first temblor, measuring 5.5 on the Richter scale, hit shortly after midnight. It was followed by a second measuring 6.2 about seven hours later. Aftershocks rattled the area, including one on Saturday afternoon with a magnitude of 5.4. "We hope that the earthquakes are settling down, but we are worried about further damage because of the heavy rain," Yoshitada Konoike, cabinet minister for disaster management, told a news conference in Tokyo. **About 130,000 homes temporarily lost electric power. Train services in the area were halted and some highways were closed. By Saturday evening, about 12,000 homes were still without water. There were no reports of damage at the Onagawa nuclear power plant in Miyagi or at nuclear plants in nearby Fukushima prefecture**, also shaken by the quake.

Source: <http://reuters.com/newsArticle.jhtml;jsessionid=NN1TRAAZYKROOCRBAELCFFA?type=worldNews&storyID=3163978>

25. *July 25, Associated Press* — **Trio of fires roar into Glacier Park. A trio of wildfires roared unchecked through parched timber and into Glacier National Park, parts of which stood deserted Friday after a mass evacuation described as "the flow of traffic like rush hour in a large city."** Even headquarters was empty at what's widely considered one of the **national park system's crown jewels**. Thousands of visitors began streaming out of the park Thursday, along with some National Park Service personnel and other park workers. Scores of residents along the park's western boundary, in the North Fork of the Flathead River drainage, also fled. "The last trip we had up to the house, we looked back and could feel the blast of the heat on our faces, the sparks rolling through the trees," said Jim Clemens, who with more than a dozen neighbors left quickly as the fire burned into the southwestern portion of Glacier. **Much of the western half of the more than 1 million-acre national park was virtually deserted by nightfall.**

Source: <http://www.cnn.com/2003/US/Central/07/25/wildfires.ap/index.html>

26. *July 25, CNN* — **Russians discover "suicide belts". Russian investigators have found a cache of explosive devices similar to so-called "suicide belts" used in a deadly double attack at a Moscow rock concert in early July.** They were working on information provided by a woman in police custody who is accused of trying to carry out a bombing at a Moscow cafe earlier this month, the agencies reported. **Six belts were found at a house in the village of Tolstopaltsevo, 30 kilometers (19 miles) southwest of Moscow, said a statement from the General Prosecutor's office. The belts were disabled by bomb experts and were being examined by explosives experts, the statement said.** A special team of FSB experts, along with investigators from the prosecutor's office, began their operation Thursday afternoon, according to an Interfax correspondent. **Interfax quoted a source as saying the design and components of the devices were identical to ones used in the July 5 rock concert bombing and at an attempted attack at a central Moscow cafe July 9 that killed a Russian demolition expert trying to defuse the bomb.**

Source: <http://www.cnn.com/2003/WORLD/europe/07/25/russia.belts/index.html>

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

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.