

**Department of Homeland Security
Information Analysis and Infrastructure
Protection**

**Daily Open Source Infrastructure Report
for 25 June 2003**

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- ABC Online reports the Financial Action Task Force, a body set up by 31 nations, now wants non-banking institutions handling money to investigate dubious accounts or clients. (See item [5](#))
- The New York Times reports the Transportation Security Administration has been tightening shoe inspections at many of the nation's airports because of new intelligence information. (See item [9](#))
- The Associated Press reports that starting July 1, any company that stores data electronically and does business in California must alert customers whenever unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (See item [18](#))

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. *June 24, Platts Global Energy News* — **Industrials call for 'war' on high natural gas prices.** A United States industrial energy users' group is asking the President George W Bush to use his emergency executive powers to "declare war on high natural gas prices." **Paul Cicio, executive director of the Industrial Energy Consumers of America, told U.S. Energy Secretary Spencer Abraham in a letter Tuesday that the use of those powers is necessary for short-term regulatory changes that would "reduce the threat of natural gas shortages and prevent sustained high price levels."** The group is recommending 13 actions, including

a moratorium on any new gas-fired power generation that does not use combined heat and power and does not meet an energy-efficient heat rate of at least 7,500 Btu/Kwh; maximizing the use of alternatives to natural gas for power generation; providing incentives to dual-fuel customers so they may switch off gas; tax credits for energy efficiency; and a federal loan guarantee program for small and mid-sized gas production and infrastructure companies.
Source: <http://www.platts.com/stories/gas1.html>

2. *June 23, Associated Press* — **Engineers discover crack in Russian nuclear reactor.** Engineers found a crack in a nuclear reactor during maintenance operations at the Novovoronezh power plant in central Russia, officials said Monday. The 3-millimeter (0.12-inch) crack was discovered in a tube in the heat exchanger of one of the plant's reactors, which had been shut down for servicing, a spokesman for the Rosenergoatom nuclear consortium said. There are 5,000 such tubes in the heat exchanger. Radiation levels at the plant remained normal, the plant's chief engineer said, according to the ITAR-Tass news agency. The reactor was to remain shut for about three more months for maintenance, ITAR-Tass said. **Earlier in June, one of the plant's reactors was shut down after a problem with a steam generator.** Russia has nine nuclear power plants with a total of 30 nuclear reactors.

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3940095

3. *June 23, Tulsa World* — **Another wind farm turns up. On 2,500 acres northwest of Lawton, OK, 45 giant wind turbines will soon be built to produce electricity — one of two major wind farms being developed in the state.** Wayne Walker of Zilkha Renewable Energy, a Houston-based company that's developing the project, said more like it are sure to be built in western Oklahoma, where the winds blow at incredible speeds. The time has come to promote more wind power development, said Steve Palomo of Wind Powering America, a U.S. Department of Energy program designed to educate potential stakeholders in wind farm projects. **The use of more wind power can help preserve the nation's dwindling supply of natural gas, which is used to generate electricity, Palomo said. The 74.25-megawatt Zilkha project will provide power to Western Farmers Electric Cooperative, which supplies 500,000 customers through 19 electric co-ops in Oklahoma.** Construction is under way, and the facility will be ready for commercial operation by year's end, officials said. **The first of 45 turbines will be raised in September. Fixed with huge fiberglass blades, each turbine will be more than 300 feet tall.**

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3940076

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

4.

June 23, Federal Computer Week — **Air Force issues \$1B RFP. The Air Force Pentagon Communications Agency (AFPCA) last week released a \$1 billion request for proposals (RFP) for a range of classified and unclassified information technology services to be used by Defense Department workers in the Washington, D.C., area.** The customer base for the 10-year, fixed-price outsourcing award is 7,500 users at Air Force headquarters, the Office of the Secretary of Defense, the Joint Chiefs of Staff, the National Military Command Center and the leadership offices of other agencies working with DOD. The RFP was released June 20, proposals are due by July 28 and an award is expected in December, according to a contract specialist working on the program. He added that the \$1 billion anticipated award "could vary by \$100 million either way." **IT services included in the RFP are e-mail, databases, Web services, an antivirus program, account and domain management, communication security, and configuration management of the common operating environment integrating more than 1,050 software applications.** AFPCA also provides voice services, video teleconferencing, cable installation, software consultation and planning, commercial off-the-shelf integration, custom software development, lifecycle support services, and a 24-hour help desk.

Source: [http://www.fcw.com/fcw/articles/2003/0623/web-afrfp-06-23-03 .asp](http://www.fcw.com/fcw/articles/2003/0623/web-afrfp-06-23-03.asp)

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

Banking and Finance Sector

5. *June 24, ABC Online* — **Non-banking institutions urged to join terrorism fight.** Suburban lawyers, estate agents, and accountants may find themselves helping in the fight against terrorism in Australia under new recommendations from an international task force looking at money laundering and the financing of terrorism. **The Financial Action Task Force, a body set up by 31 nations including Australia, now wants non-banking institutions handling money to investigate dubious accounts or clients. It's estimated that as much as \$1.5 trillion, or five per cent of global gross domestic product is laundered via various complex financial schemes.** And while it's not clear how much of that is directly linked to terrorism, an international body of officials and experts from some 31 countries has developed 40 recommendations in the battle against this crime.

Source: <http://www.abc.net.au/worldtoday/content/2003/s886102.htm>

6. *June 24, Reuters* — **West Virginia sues ten Wall Street firms. West Virginia's attorney general Tuesday said he filed suit against 10 Wall Street firms, claiming relationships between banking and research departments represented an illegal conflict of interest under state law.** The complaint filed by Attorney General Darrell McGraw comes two months after a record \$1.4 billion global settlement with those same firms following New York Attorney General Eliot Spitzer's probes of stock research by Wall Street analysts. **West Virginia seeks more than \$300 million in damages based on its Consumer Credit and Protection Act.** The state is suing on behalf of residents who may have made investment decisions based on what it alleged could be biased research issued by the firms' analysts.

Source: <http://www.msnbc.com/news/930676.asp?0cv=BA00>

7. *June 24, Reuters* — **Fed set to cut rates. The U.S. Federal Reserve, seeking to rev up a slow recovery while keeping price deflation at bay, is universally expected to cut interest rates**

to 1958 lows this week. The sole mystery surrounds whether the 13th in a long line of rate reductions, expected to be announced on Wednesday, will be a quarter or bolder half percentage point. Fed Chairman Alan Greenspan set the wheels in motion for a rate drop before Congress on May 21 when he talked about "taking out insurance" against deflation and weak demand. Talking to fellow central bankers in Berlin earlier this month, he said deflation would be discussed "in some considerable detail" at this two-day meeting of the policy-setting Federal Open Market Committee.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A24905-2003Jun 24.html>

[[Return to top](#)]

Transportation Sector

8. *June 24, Post Dispatch (St. Louis)* — **Rail crossing safety would lose status in bill.** The White House's proposed federal transportation spending plan could spell the end of the line for a program aimed at preventing accidents at the nation's railroad crossings. **Under the plan, the administration would no longer require states to spend \$155 million a year of their federal transportation aid on rail highway crossings.** Missouri's share of the federal money is about \$4 million annually, while Illinois receives about \$8 million. **Instead, the crossing money – distributed until now under the federal government's Section 130 program – would go to the states in a form that would give them greater latitude in how it is used to improve transportation safety.** Not long after Secretary of Transportation Norman Mineta unveiled the transportation spending proposal last month, a railroad trade association voiced concern about elimination of the Section 130 program. While not a significant line item in any state highway budget, industry officials say the rail highway crossing program has helped in significantly reducing the carnage at the nation's crossings over the past three decades. **Between 1975 and 2002, the number of collisions at highway rail grade crossings plunged from 12,126 to 3,066. The number of crossing deaths was cut by more than half over that span, too, from 917 to 35**

Source: <http://www.stltoday.com/stltoday/news/stories.nsf/News/F6D91FC5CE582BC786256D4F00187374?OpenDocument&Headline=Rail+crossing+safety+would+lose+status+in+bill>

9. *June 24, New York Times* — **Shoe inspections leave passengers fit to be untied.** Suddenly, the issue of having to take off one's shoes at security checkpoints is a hot one, coming many months after most business travelers and other frequent fliers, who pride themselves on sailing through checkpoints, had adopted other forms of footwear: sneakers, sandals, moccasins and the like, that did not contain the metal supports that trigger alarms. **Just as summer air travel is picking up, the federal Transportation Security Administration (TSA), citing new intelligence information, has tightened procedures over shoe inspections at many of the nation's airports. At these airports, you now have to put your shoes through the X-ray machine even if you have worn them through the security area a thousand times without setting off the magnetometer alarm, even booties on your infant's tiny feet.** The TSA has been tightening shoe inspections because of new intelligence information, said Brian Turmail, an agency spokesman. He said he could not describe the nature of any threats, **but added that the all-shoes-off policy was being applied only at certain airports.** "Folks have called us and we've explained to them that although we can't cite specific reasons for it, we have made

some changes to our shoe-screening process," he said. "Those are temporary changes, and as the nature of the threat information we receive changes, so too will our process."

Source: <http://www.nytimes.com/2003/06/24/business/24ROAD.html>

10. *June 23, The Cincinnati Enquirer* — **Driverless trains carry future of rail industry.** Paul Wells eased the lever forward a bit and released the brake button on his remote control, sending a 3,000-horsepower, 200-ton driverless diesel-electric locomotive at the company's Queensgate Yard facility using a neon green "belt pack." Wells then passed control of the train to his co-worker several hundred yards down the track. **Throughout the 160-acre yard, one of the most important switching facilities in the Midwest's rail network, such remote operators, who help shuttle cars from incoming trains to outbound trains bound for destinations to the south and west, control most of the engines at the yard near downtown Cincinnati.** It's one of the innovations and equipment investments that CSX specifically and the \$36 billion railroad industry in general are making to boost safety and efficiency. CSX officials say that the remote technology, which gained widespread use in Canada 10 years ago, has improved safety. **There has been a 60 percent reduction in accidents since CSX began training classes last October. The company now uses the technology in about 75 locations, and plans to add remote control to engines in an additional 63 this year.**

Source: <http://www.clarionledger.com/news/0306/23/b02.html>

11. *June 23, Reuters* — **NATO is hunting 20 suspect ships on terror list.** NATO naval forces, which tipped off Greece to a ship in its waters carrying 680 tons of dynamite, said on Monday they were hunting 20 suspect vessels that intelligence trackers say could be used by terror groups. "It's in the order of 20: a moving list, moving target. Vessels fall off it and vessels join it," Lieutenant Commander Harvey Burwin, a spokesman for Operation Active Endeavour, said. Active Endeavour is a maritime anti-terror operation that began in October 2001 and covers the Mediterranean Sea. **"The Contact of Interest list are vessels which have achieved a level of suspicion by numerous intelligence sources and if they fell within our level of interest there is a possibility that they would be boarded and searched,"** Burwin said. **"We look for ships that have had frequent changes of flag and ownership."**

Source: <http://www.nytimes.com/reuters/international/international-security-ships.html>

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

12. *June 24, Daily Republic* — **Parasite found near nut tree.** County farming officials are beefing up inspections and asking for the public's help after a deadly pest known for its devastating impact on grape crops was found in Vacaville, CA. State agriculture scientists on Monday confirmed an insect found near the Nut Tree was a glassy-winged sharpshooter. Officials believe the insect was brought to the county on nursery stock. **County Agriculture**

Commissioner Susan Cohen said there is no evidence of an infestation. More sharpshooters could spell trouble for a whole range of crops, including wine grapes, citrus fruit and alfalfa. Besides robbing leaves of life-giving fluids, the pests transmit Pierce's Disease, which can kill plants when spread.

Source: <http://www.dailyrepublic.com/articles/2003/06/24/news/news3.txt>

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

Food Sector

13. *June 20, Federal Computer Week* — USDA launches online grocery. The U.S. Department of Agriculture (USDA) has completed the nationwide launch of an online grocery store for such state programs as school lunches and emergency food assistance. **The Electronic Commodity Ordering System allows state officials to order nonperishable foods online, replacing a paper-based or electronic data interchange system.** With the system, the USDA has a clear understanding, for example, of each school district's needs and a grasp on which commodities are in demand. The system was piloted in California, Connecticut, Illinois, and Virginia, and launched nationwide in mid-March. **It now serves 76 state agencies and about 1,000 users.**

Source: <http://www.fcw.com/fcw/articles/2003/0616/web-usda-06-20-03.asp>

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

Water Sector

Nothing to report.

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

Public Health Sector

14. *June 24, Reuters* — WHO lifts Beijing SARS travel warning. The World Health Organization (WHO) declared the Chinese capital free of the spread of Severe Acute Respiratory Syndrome (SARS) on Tuesday and lifted its warning against travel to Beijing. **Beijing was the last remaining area in the world subject to a WHO travel warning because of SARS.** The announcement underscored the turnaround in Beijing which was blamed widely for concealing the scale of contagion for weeks before confronting it head on and mobilizing the masses. Beijing has had more than 2,500 cases of the flu-like illness and more than 190 deaths, but has gone 13 days without any new confirmed infections.

Source: <http://reuters.com/newsArticle.jhtml?type=scienceNews&storyID=2977868>

15. *June 24, Associated Press* — House panel ponders counterfeit drug problem. A House panel Tuesday will hear about what it bills as "an avalanche" of counterfeit and unapproved drugs that are overwhelming the system. In the past seven years, the U.S. Food and Drug Administration has investigated 71 cases of fake drugs and made 43 arrests. But the problem appears to be growing. **The committee will hear from several officials from Florida, where three men recently pleaded guilty in a scheme to pass off bacteria-tainted**

water as Procrit, an expensive drug used to fight severe anemia.

Source: <http://www.thejacksonchannel.com/health/2289820/detail.html>

16. *June 23, CIDRAP News* — **NIAID offers genome of SARS virus on chip.** The National Institute for Allergy and Infectious Diseases (NIAID) announced Monday that it will offer a quartz chip containing the DNA of the Severe Acute Respiratory Syndrome (SARS) virus to help researchers quickly detect differences between strains of the virus. **"NIAID has purchased several hundred microarrays, a reference strain of the SARS coronavirus embedded in a quartz chip, and will distribute the arrays at no cost to qualified researchers worldwide,"** the agency said in a news release. In the announcement, NIAID Director Anthony S. Fauci said, "This powerful tool will help us better understand this newly recognized pathogen and its spread, and will provide new leads in our search for effective SARS countermeasures." **The array, designed with data from several research centers that sequenced the SARS coronavirus genome, includes the virus's 29,700 DNA base pairs.**

Source: http://www.cidrap.umn.edu/cidrap/content/hot/sars/news/june2_303chip.html

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

Government Sector

17. *June 24, Federal Computer Week* — **OPM speeds hiring of cyber specialists.** All executive branch agencies are free to hire their own information technology professionals to bolster the security of their information systems, the Office of Personnel Management (OPM) has announced. **The agency notified agency heads and chief human capital officers of the new direct-hire authority, effective immediately, for professionals in the GS-2210 series at Grade 9 and above. The announcement is intended to speed hiring of cybersecurity specialists.** For a number of years, agencies have found it difficult to hire and retain IT specialists. The shortage has been mitigated in recent months by downturns in the IT industry and other industries that employ IT workers, as well as special increases in pay for those in the 2210 series, which covers IT management jobs. **However, the push for greater homeland security has increased the demand for qualified cybersecurity specialists.** Congress enabled OPM to increase hiring flexibility when it enacted the Homeland Security Act of 2002.

Source: <http://www.fcw.com/fcw/articles/2003/0623/web-hire-06-24-03.asp>

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

Emergency Services Sector

Nothing to report.

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

Information and Telecommunications Sector

18. *June 25, Associated Press* — **California law forces firms to warn consumers of hacking events.** Starting July 1, companies must warn California customers of security holes in their corporate computer networks. **Any company that stores data electronically and does**

business in California must alert customers whenever "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The bill defines "personal information" as an individual's first name or initial and last name, with one of the following: Social Security number; driver's license number; state identification number; or credit or debit card account number and security code. Local politicians call the regulation the first of its kind in the United States, and it could become the model for a nationwide law.

Proponents say the California bill makes executives more accountable for computer fraud. It doesn't impose specific monetary fines, but **the regulation makes companies with questionable computer networks more vulnerable to lawsuits and public scorn.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A22227-2003Jun 23.html>

19. *June 23, Associated Press* — **Feds form anti-terror e-posse. A partnership called the Infragard program has developed between the FBI and 8,300 companies to share information about both cyber and physical threats.** On Monday, experts from around the country were expected to gather for the program's first national conference in Washington, D.C. The program, started in 1996, was growing slowly but steadily until the terrorist attacks of September 11, 2001, made security the top priority for the FBI. "When Wall Street was shut down, banking was hit very hard, transportation was hit very hard – they're all part of the infrastructure we're trying to shore up and protect," said Brett Hovington, the FBI's national coordinator of the Infragard program. Hovington says **the program allows the FBI to detect patterns that could alert the agency to a terrorist threat.** The FBI and companies emphasize that **the Infragard program is voluntary and they do not share information such as confidential personnel records protected by privacy laws.**

Source: <http://www.cbsnews.com/stories/2003/06/23/attack/main559834.shtml>

20. *June 19, IDG News Service* — **Africa confronts cybercrime. Law enforcement agencies and ISPs (Internet service providers) in Africa are trying to stem a wave of cybercrime originating from some parts of the continent.** Credit card "cloning" and e-mail scams are the main types of cybercrime, according to Isaac Prah of the Criminal Investigation Department (CID) of the Ghana Police Service. **Members of the African Working Party on Information Technology Crime—a law enforcement community that collaborates in sharing knowledge and experiences in information technology crime—are lobbying legislators in their countries to enact laws that can be used to prosecute cybercrime.** "You cannot prosecute someone for misusing a computer," Prah said, in discussing Ghana's current laws. Organized criminal gangs normally use cybercafes to carry out credit card fraud, Prah and other officials said. In addition, staff in hospitality and other service industries may pass on the credit card details of a client they serve to criminals with whom they are in collusion.

Source: http://www.idg.net/ic_1322277_10320_1-5073.html

Internet Alert Dashboard

| Current Alert Levels | |
|--|--|
|  AlertCon: 1 out of 4 https://gtoc.iss.net |  Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/ |
| 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 | 137 (netbios-ns), 80 (www), 1434 (ms-sql-m), 445 (microsoft-ds), 4662 (eDonkey2000), 113 (ident), 139 (netbios-ssn), 6346 (gnutella-svc), 0 (----), 25 (smtp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center |

[[Return to top](#)]

General Sector

21. June 24, CNN — Arizona wildfire tops 20,000 acres. Firefighters made progress battling a 20,000-acre wildfire in mountainous southern Arizona overnight, authorities said, but the blaze still was spreading north and east early Tuesday. **More than 900 people are battling the Aspen wildfire, northeast of Tucson, and the blaze was 15 percent contained, said Rick Barton, a spokesman for the interagency group trying to suppress the fire. But with forecasters predicting another dry, gusty day, Barton said firefighters were wary.** The week-old wildfire has destroyed more than 200 homes and businesses so far -- many of them in the vacation community of Summerhaven and nearby Loma Linda, which the flames swept through last week. **Smoke and flames from the mountaintop can be seen in nearby communities such as Oracle, about five miles north of the Aspen fire, and Catalina, about five miles to the west. But no communities are in imminent danger,** Barton said. More than 1,000 homes and a number of children's camps have been evacuated since the fire began June 17. Residents probably will not be able to return to their homes for at least a week, officials said. **The cause of the wildfire is not known, since investigators are unable to approach the area where it is believed to have started.**

Source: <http://www.cnn.com/2003/US/Southwest/06/24/arizona.wildfire/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 202-324-1129

Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov 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.