

**Department of Homeland Security
Information Analysis and Infrastructure
Protection
Daily Open Source Infrastructure Report
for 02 July 2003**

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Sydney Morning Herald reports influenza could easily be turned into the next weapon of mass destruction, since it is readily accessible and the possibility for genetic engineering and aerosol transmission suggests an enormous potential for bioterrorism. (See item [11](#))
- The Register reports a recent post on the Bugtraq mailing list has revealed a serious flaw in the core design of the personal firewall ZoneAlarm running on Microsoft Windows. (See item [16](#))
- IDG News Service reports a newly disclosed vulnerability could let attackers reset passwords and hijack older Microsoft .Net Passport accounts. (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 30, Fairfield County Business Journal (CT)* — **Cross-Sound Cable, LIPA offer power carrot.** The owners of a controversial underwater power cable that connects southwestern Connecticut to Long Island say they believe the cable would help ensure the reliability of the state power supply if the state allowed them to flick the switch. But state officials say they are not convinced. **They are holding Cross-Sound Cable Company LLC to the terms of its permit which says the cable must be buried at least 48 feet below the seabed – before allowing it to be turned on.** "We've continued to remind them that meeting the environmental standards set forth in their permit is of the utmost importance right now," said Michele Sullivan, spokesperson for Gov. John G. Rowland. Jeffrey A. Donahue, chief executive officer

of Cross–Sound Cable, made an offer in a statement released May 8 where the Long Island Power Authority would sell energy to Connecticut over the next four years in exchange for the Cross–Sound and the Norwalk–Northport Cable being opened up immediately. **Local utilities and New England's Independent System Operator (ISO) say the electric transmission lines that currently run into the southwest portion of the state cannot support the high voltage electricity produced by today's more modern and efficient plants. As a result, it costs more to bring energy from older, less efficient plants to Fairfield County.**

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3958069

- 2. *June 30, The Virginian–Pilot (Norfolk, VA)* — Dominion hopes to join regional power grid.** The company that owns Dominion Virginia Power filed for state regulatory approval to turn over its transmission system to the operator of the power grid crossing from the Midwest to the Mid–Atlantic states. **Dominion Resources Inc. filed its application to the State Corporation Commission on Friday, outlining cost benefits that both the company and its customers would see if it joined its 6,000 miles of power lines to PJM Interconnection.** PJM, an independent entity known as a regional transmission organization, or RTO, would give Dominion customers access to excess electricity produced across a larger geographic area, helping to lower costs, Dominion officials said. **PJM, based in Pennsylvania, oversees wholesale transactions between power generators and power users or companies buying it on behalf of consumers. It works to ensure that all players have equal access to the electricity highway.** The Federal Energy Regulatory Commission has pushed for the formation of regional transmission operators to create a seamless flow of power across state borders and utility territories. Without the regional organization, a power purchaser would have to pay fees to several utilities to move electricity from a producer in Ohio, for example, to consumers in Virginia.

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=bhsuper_2003_06_28_NFLK_0000-4557-KEYWORD.Missing&SMContentSet=0

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

Nothing to report.

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

Banking and Finance Sector

- 3. *July 01, Knight Ridder* — Banks slower to implement latest interest rate cut.** On 12 occasions beginning in 2001, the Federal Reserve lowered interest rates. And each time, banks rushed to pass along the decrease to borrowers within hours, or even minutes, after the Fed's

announcement. **But when the Fed lowered the federal funds rate for the 13th time Wednesday, the banking world flinched. Bank of America did not cut rates until the financial markets closed Thursday. Wachovia, BB&T, and First Citizens Bank of Raleigh waited until Friday. Central Carolina Bank held out until Monday afternoon. Capital Bank will lower its prime rate today. The delay could be a hint of things to come if the Fed decides to reduce rates further, say analysts. Faced with shrinking profits, some banks may choose to ignore any future rate cuts by the Fed.** "You get to a point where lower rates really crush bank profits," said Karen Dorway, president of BauerFinancial, a bank rating and research firm. "That's when banks start to resist."

Source: http://www.wokr13.tv/business/story.aspx?content_id=8534D017-0A1C-4A79-BC93-D28769C2AC43

4. *July 01, Manila Times* — **Revised antimoney laundering rules. The committee tasked with overseeing implementation of the Anti-Money Laundering Act (AMLA) has approved the revised guidelines of the law, thus helping pave the way for the Philippines' removal from an international blacklist of dirty money havens.** A majority in the Congressional Oversight Committee, five members of the Lower House panel, and four senators have endorsed the draft implementing rules and regulations of the AMLA. Although the AMLA is self-executory, the implementing rules could strengthen a provision in the law authorizing bank examiners to look into deposits or investments without need for a court order. **Under Section 11 of the law, the AMLC can look into "any particular deposit or investment with any banking institution or non-bank financial institution without a court order" when it involves any of the three unlawful activities, namely, kidnapping for ransom, drug trafficking, and hijacking.**

Source: http://www.manilatimes.net/national/2003/jul/02/business/200_30702bus1.html

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

Transportation Sector

5. *July 01, Associated Press* — **Firecrackers can set off airport security.** Anyone who plans to set off fireworks on the Fourth of July, be forewarned: your pyrotechnics may delay you at the airport later. Ultrasensitive equipment that can detect minuscule traces of explosives on suitcases and skin might raise suspicions at the security gate. **Ever since federal security screeners began checking baggage for weapons and bombs at airports last year, they've been discovering suspicious substances used for innocent purposes on air travelers' luggage. Fertilizer, for example, can activate an alarm. That's why the Transportation Security Administration warns golfers to clean their shoes and clubs before heading to the airport.** Susan Hallowell, director of the TSA's security laboratory, said **the equipment has detected residue on police officers after they've come off firing ranges, on people who set off avalanches for a living and on heart patients who take nitroglycerin tablets.** "The bad news is you get nuisance alarms," said Randal Null, the TSA's chief technology officer. "The good news is the equipment is doing what it's supposed to do."

Source: <http://www.cnn.com/2003/TRAVEL/07/01/airports.fireworks.ap/index.html>

6. *July 01, Government Executive Magazine* — **Homeland department unveils new port security regulations. The Department of Homeland Security (DHS) on Tuesday announced new regulations for port and vessel security, requiring security plans for**

commercial vessels ranging from cruise liners to cargo ships and approximately 5,000 ports and other facilities. The rules are part of the department's implementation of a 2002 maritime transportation security law. Asa Hutchinson, DHS undersecretary for transportation, and Vice Admiral Thad Allen of the U.S. Coast Guard announced the publication of the new rules, which were written after the department held seven public meetings nationwide, and they are intended as flexible guidelines for ports of different sizes and functions to meet the same security requirements. **However, the rules will require more ships to carry Automatic Identification System (AIS) technology. These "black box" devices transmit ship speed, destination and identification to other ships and to shoreside monitoring stations. Additionally, the new order is intended to provide instantaneous identification of all large ships in U.S. waters.** These rules are effective immediately on an interim basis, with public comments accepted for the next 30 days. Final regulations will be published in October, and ships and ports must implement their security plans by July 2004. Source: <http://www.govexec.com/dailyfed/0703/070103td1.htm>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

7. *July 01, Wisconsin Ag Connection* — **Federal lawmakers establish grants to help fight CWD.** U.S. Senator Russ Feingold, Representative Mark Green, and Representative Paul Ryan joined together last week to introduce legislation, in both the Senate and the House, creating three new grants aimed at helping states fight Chronic Wasting Disease (CWD). These grants will make a total of \$20.5 million available to states and tribal governments to combat the disease. **The legislation will allow states and tribal governments to apply for three separate grants, including \$10 million will be available to states with CWD outbreaks; \$7.5 million will be available to all states; and \$3 million will be available to tribal governments.** Source: <http://www.wisconsinagconnection.com/story-state.cfm?Id=788&yr=2003>

8. *July 01, Ventura County Star* — **Newcastle quarantines lifted. Officials with the exotic Newcastle Disease Task Force said Monday that quarantines in Simi Valley, CA have been lifted, although the restrictions against transporting birds across county lines remain in effect.** Bird owners under quarantine received information in the mail Friday, notifying them that bird breeding and routine activities, such as visits to a veterinarian with pet birds, could return to normal. Three homes in Simi Valley were quarantined on March 31 and April 1 after an outbreak of the disease was discovered among a backyard flock. **Larry Cooper, spokesman for the joint task force of the state Department of Food and Agriculture and the U.S. Department of Agriculture, said samples taken from birds in eight counties in Southern California are being tested and may result in lifting the statewide quarantine by the end of July.** Source: http://www.insidevc.com/vcs/sv/article/0,1375,VCS_239_207972_0,00.html

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

Food Sector

9. *July 01, Crop Decisions* — **USDA will increase enforcement of inspection acts. U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) issued a notice that it intends to increase enforcement of the registration and recordkeeping requirements of the Poultry Products Inspection Act (PPIA) and the Federal Meat Inspection Act (FMIA).** Since 1970, FSIS has required businesses affected by PPIA and FMIA to maintain business records and to make the records available to FSIS employees upon request. **As a part of the increased enforcement, the agency has developed a new registration form that asks registrants to provide certain information that was not requested previously, including an e-mail address, phone number, and subsidiaries' hours of operations.**
Source: http://www.cropdecisions.com/show_story.php?id=20184

10. *June 30, Agriculture Online* — **USDA mulls new measures to prevent mad cow disease.** There is a good chance new safeguards will soon be imposed on meat processors to protect Americans from mad cow disease, or BSE, the U.S. Agriculture Department (USDA) said on Monday. **The U.S. is considering a blanket ban on cattle brains and spines from being used in food and animal feed.** "There is a good chance we will enhance our systems here," USDA spokeswoman Alisa Harrison said. "We are just determining what the science tells us what they should or could be." Japan, the top U.S. beef buyer, and South Korea have demanded the United States tighten its mad cow protections. **A U.S. ban could end a meat processing system, known as advanced meat recovery, that is used by most large U.S. beef companies.** The equipment strips beef from cattle bones and can inadvertently leave bits of spinal cord and brain tissue in sausages, hamburgers, and taco meat. **Jan Novakofski, animal health expert at the University of Illinois, said a blanket ban would weigh heavily on the industry without any significant consumer benefit.** "While the benefits are small, the costs to the industry would be large as they would need to decide how to get rid of large amounts of prohibited product," he said.
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=goDe tail_ANewsindex_html_50183_1

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

Water Sector

Nothing to report.

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

Public Health Sector

11. *July 01, Sydney Morning Herald* — **Flu could be next terror weapon, warn scientists.** Influenza could easily be turned into the next weapon of mass destruction, scientists said Monday. **Taken together with the fact that influenza virus is readily accessible and may be**

causing more deaths than previously suspected, the possibility for genetic engineering and aerosol transmission suggests an enormous potential for bioterrorism," the University of Texas scientists said. The team led by Dr. Mohammed Madjid noted that last century a series of 'flu epidemics from Spain to Russia and Hong Kong had killed millions of people as the virus naturally mutated. They pointed out that sequencing of the genome of the 1918 Spanish 'flu epidemic was nearly complete, opening the door to unscrupulous scientists to build an even more potent virus. **"Recently, the possibility of synthesising an infectious agent solely by following instructions from a written sequence has moved from theory to practice."** The scientists also noted that while infection generally took place through personal contact, the disease was also easily transmissible through tiny droplets in the air.

Source: <http://www.smh.com.au/articles/2003/07/01/1056825375795.html>

12. *July 01, Japan Today* — **Japan to get more SARS virus strains. Japan is expected to receive corona virus strains from several more SARS-hit areas in Asia in an effort to develop a vaccine for Severe Acute Respiratory Syndrome (SARS), health minister Chikara Sakaguchi said Tuesday.** The areas including Taiwan, the Philippines, and Vietnam, gave positive responses to Japan's request in bilateral talks held on the sidelines of a meeting of health ministers of the Asia-Pacific Economic Cooperation forum in Bangkok late last month, Sakaguchi told a press conference.

Source: <http://www.japantoday.com/e/?content=news&cat=1&id=264945>

13. *June 30, Reuters* — **Irish scientist discovers new strain of AIDS virus. An Irish scientist has discovered a new strain of HIV, the virus that causes AIDS, which may provide vital clues in the hunt for a vaccine.** University researcher Grace McCormack came upon the previously unknown virus type while researching blood samples from Malawi, dating back from the early years of the AIDS epidemic in the 1980s. **"It is very interesting because while we have found people infected with it in the 1980s, we haven't found any examples of it in the 1990s yet,"** said McCormack, a lecturer at the National University of Ireland. **"As a result, it might be a strain of the virus that has failed. Because of that it may give us information on how to defeat the virus."** There are nine known strains of HIV, the virus that causes AIDS.

Source: <http://asia.reuters.com/newsArticle.jhtml?type=scienceNews&storyID=3013535>

[[Return to top](#)]

Government Sector

14. *July 01, Associated Press* — **California and six states fail to reach budget deal. For the third consecutive year, California began the new fiscal year Tuesday without a state budget after lawmakers were unable to break a partisan impasse over spending and taxes. Six other states also took their budget deliberations to the June 30 deadline without reaching a final agreement.** Lawmakers in Oregon, New Hampshire and Connecticut approved short-term spending plans allowing government to operate while debate continued. Residents in Nevada, New Jersey and Pennsylvania began Tuesday without a new budget. In Massachusetts, Gov. Mitt Romney signed a \$22.1 billion state budget on the final day of the fiscal year, the first time in seven years a budget has been completed on time. He then immediately issued \$201 million in vetoes, including a \$23 million cut in additional assistance to cities and towns. **But nowhere are the stakes higher than in California. The state faces a**

record \$38.2 billion budget shortfall and is operating for the first time completely on borrowed money. State Controller Steve Westly says the state only has enough cash to get through mid–August, and officials say the state cannot borrow any more until a new budget is passed. Without a new budget by the deadline, the state is unable to legally make millions of dollars in on–time payments to schools, community colleges, courts, state suppliers and others. Source: <http://www.cnn.com/2003/ALLPOLITICS/07/01/state.budgets.ap/index.html>

[[Return to top](#)]

Emergency Services Sector

15. *July 01, The Raton Range (New Mexico)* — New Mexico unit trains for handling terrorism incidents. From unknown chemicals at the Armex building to an explosion at the fire department's training tower, Raton, NM came under terrorist attack last week. Thankfully, it was only for training purposes. Any weapons of mass destruction were not real. However, the special New Mexico National Guard unit that was taking part in the exercise is quite real. And its members were training for a situation they hope never happens. **The 64th Civil Support Team of the New Mexico Army/Air National Guard is specially trained to handle incidents involving weapons of mass destruction. The team's 22 members hold training exercises in different communities throughout the state so they can work with local emergency responders during training exercises.** The full–time National Guard unit worked out in Raton last week under the watchful eyes of Army evaluators. A special unit from San Antonio, Texas, was present at the exercises to evaluate and critique the performance of the New Mexico unit based in Santa Fe. The unit is evaluated about every year and a half. **The 64th Civil Support Team is the lone unit of its kind in New Mexico. Nationwide, there are 32 such teams training to deal with weapons of mass destruction. Plans for 23 more teams are in the works.**

Source: <http://www.ratonrange.com/RATONRANGE/myarticles.asp?P=595410&S=318&PubID=9505>

[[Return to top](#)]

Information and Telecommunications Sector

16. *June 30, The Register* — ZoneAlarm bells ring over freeware flaw. A recent post on the Bugtraq mailing list has revealed **a serious flaw in the core design of the personal firewall ZoneAlarm running on Microsoft Windows.** ZoneAlarm could theoretically be tweaked into opening an unsecured Internet connection and leaking information into web servers anywhere. By introducing a Trojan into a user computer, hackers could theoretically force an Internet connection bypassing the security of the freeware firewall, provided that the affected user clicked on the product's pop ups without reading them. Although the attack has yet to be deployed in the wild, **it could potentially be used to bypass the security of the freeware version of ZoneAlarm and leave millions of users data exposed. ZoneLabs points out that the bug was only tested on version 3.1 of ZoneAlarm (it is now up to 3.7). ZoneLabs is currently working to resolving this bug.**

Source: <http://www.theregister.co.uk/content/55/31481.html>

17. *June 30, Computerworld* — **General Clark wants more proactive government role in cybersecurity.** Retired supreme allied commander General Wesley K. Clark told hundreds of government and private-sector representatives Monday that **a better balance between market incentives and government regulation is urgently needed, particularly in the areas of cybersecurity and critical-infrastructure protection.** Clark's comments were made in Philadelphia during the Government Symposium on Information Sharing and Homeland Security. **"To make the standards work in the private sector, you start with insurance and with the federal government underwriting risks. [However], there may be areas where you can't do that and you simply have to mandate it and say that in order to be licensed as a business, you must meet certain standards," he said.** Clark said there is little or no incentive for the private sector to move away from the current security model, which is centered on not reporting security incidents.
Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,82646,00.html>
18. *June 30, IDG News Service* — **Microsoft security service said to allow some account hijackings. A newly disclosed vulnerability could let attackers reset passwords and hijack older Microsoft .Net Passport accounts,** according to a message on an online mailing list. .Net Passport enables customers to use a single e-mail address and account password to sign on to a variety of affiliated services and Web sites including the Hotmail e-mail service. **Microsoft has implemented a Secret Question feature to validate the identity of a user who needs to reset an account password.** But according to the security list discussion, **attackers can manipulate this feature on .Net Passport accounts that were set up before Microsoft implemented the Secret Question function.** To take advantage of the vulnerability, an attacker must know both the e-mail address and the home country of the account owner. In the case of U.S.-based accounts, an attacker also needs the state and the zip code of the account owner. **Microsoft did not immediately respond to requests for comment.**
Source: <http://www.pcworld.com/news/article/0,aid,111403,00.asp>
19. *June 24, Federal Computer Week* — **City tries new path to fiber network. San Francisco is the first U.S. local government customer for a system that uses existing sewer systems to build fiber-optic networks.** Developed and commercialized by Vienna, Austria, the system strings fiber-optic cable through a city's sewers as an alternative to ripping up streets to lay cable. **In sewers too narrow for people to access, robots navigate the pipes and perform installations.** The San Francisco city and county are building a two-mile, fiber-optic pilot project. The project will connect additional facilities to E-Net, the city-owned, conventional fiber-optic network that links government buildings.
Source: <http://www.fcw.com/geb/articles/2003/0623/web-fiber-06-24-03.asp>

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_KLEZ.H 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), 7345 (swx), 139 (netbios-ssn), 113 (ident), 0 (----), 9007 (----), 6346 (gnutella-svc) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

20. *July 01, Associated Press* — **Extra police to heighten New York's security for 4th of July. More than 4,000 extra police officers will be on patrol throughout the city to provide a deterrent to illegal fireworks, drunk driving and would-be terrorists during the Fourth of July holiday weekend.** Police commissioner Ray Kelly said both plainclothes and uniformed officers will be part of the city's anti-terrorism security detail. "We have no specific threats targeting the city," Kelly said during a press conference held along with Mayor Michael Bloomberg. "In terms of security, we think New Yorkers should relax and let our law enforcement professionals do the worrying for us," Bloomberg added. **Police officers will set up drunk driving checkpoints throughout the five boroughs and on adjacent waterways and will also increase highway patrols.**
 Source: <http://www.newsday.com/news/local/wire/ny-bc-ny--holidaysecurity0701jul01.0.3139091.story?coll=ny-ap-regional-wire>

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

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.