

**Department of Homeland Security
Information Analysis and Infrastructure
Protection**
**Daily Open Source Infrastructure Report
for 14 May 2003**

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The U.S. Department of the Treasury has announced a newly designed twenty dollar bill, the purpose of which is to stay ahead of those who would compromise the security and integrity of the bill through counterfeiting. (See item [8](#))
- The U.S. Attorneys Office, Camden, New Jersey announced seven suspects were arrested in early morning raids on Friday; they are major players in an organization producing over \$10 million worth of fictitious money orders that appeared to be issued by the federal government. (See item [10](#))
- Federal Computer Week reports the U.S. Bureau of Customs and Border Protection is stepping up security on the border with Canada by deploying intelligent software for hundreds of video cameras that can see and analyze unusual activities or movements in real time. (See item [13](#))
- The Register reports that an Internet worm called "Fizzer," which can spread via e-mail as well as over file sharing networks, has key logging and Trojan functionality. (See item [25](#))

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. *May 13, Platts Global Energy News* — **Damaged Hungarian nuclear plant fuel might be linked to tank design. Damage to 30 fuel assemblies at the Paks Nuclear Power Plant, near the Hungarian town of Paks, was due to a deficient design of the closed fuel cleaning tank**

cooling and control system, Paks Nuclear Power Plant Ltd. said in an English-language statement issued May 12 on the its Web site (www.npp.hu). However, the Hungarian Atomic Energy Authority (HAEA) said that the plant report, which it received May 10, lists "numerous" reasons for the April 10 incident. **The root-cause investigation is ongoing. A senior HAEA official said that the design for removing residual heat from the container holding the fuel after chemical decontamination was cited as a "probable" cause. The design didn't take into account holes at the top and bottom of the VVER-440 fuel assemblies that let cooling water bypass the assemblies, leading to overheating when the fuel was left longer than expected in the container**, he said. Framatome ANP GmbH, which designed the system and conducted the decontamination, said it was "surprised" by Paks General Manager Istvan Kocsis' declaration May 12 that the company was responsible for the incident. Kocsis added, however, that Paks' own verification systems hadn't detected the design problem

Source: <http://www.platts.com/stories/nuclear1.html>

2. *May 13, Platts Global Energy News* — **Russia says will attend OPEC's June 11 meeting.** Russia will send a representative to OPEC's June 11 meeting in the Qatari capital Doha, Moscow's energy minister Igor Yusufov said Tuesday. **Speaking after talks with visiting OPEC president Abdullah al-Attiyah, who is also Qatar's oil minister, Yusufov said it was essential for OPEC to coordinate its activities both with the world's main oil consuming nations and with independent oil producers. As well as Russia, OPEC has invited independent producers Angola, Egypt, Mexico, Norway, Oman and Syria to its June 11 conference.** Norway has turned down the invitation. **Russia—the world's biggest oil producer after OPEC powerhouse Saudi Arabia, accounting for around 10% of the oil traded on international markets—often attends OPEC meetings as an observer.** Attiyah last week said OPEC "must implement new reductions in its production" because there was "too much oil on the market." He said OPEC alone could not stabilize oil markets, calling on independent producers to act alongside the oil producers' cartel in the interests of price stability.
Source: <http://www.platts.com/stories/oil1.html>
3. *May 13, Platts Global Energy News* — **SMD to save consumers \$1-bil/yr over six years.** The U.S. Federal Energy Regulatory Commission's (FERC) standard market design (SMD) plan should save electricity consumers roughly \$1-bil per year in the first six years the plan is in effect, the Department of Energy said Tuesday. **In its long-awaited cost-benefit analysis, DOE also estimated that a few regions—mostly in the Southwest—could see near-term wholesale price increases, but over the long run, all consumers should receive net benefits.** The study said SMD would improve electricity trade across the country, spreading the costs of lower cost generation to more consumers. "Greater trade means more displacement of high-cost generation, resulting directly in lower total fuel costs," the study said.
Source: <http://www.platts.com/stories/electricpower1.html>
4. *May 13, General Accounting Office* — **GAO-03-483: Nuclear Nonproliferation: DOE Action Needed to Ensure Continued Recovery of Unwanted Sealed Radioactive Sources.** **The General Accounting Office did this study because potentially dangerous sealed sources containing greater-than-Class-C radioactive material pose a threat to national security, since terrorists could use them to make "dirty bombs."** GAO was asked to determine the number of unwanted sealed sources that the Department of Energy (DOE) plans

to recover through 2010 and the estimated cost, the possible problems, and the status of efforts to provide a disposal facility. Among other recommendations, the GAO suggests that **the Secretary of Energy determine if the priority of the project is commensurate with the threat the sources pose, take immediate action to provide space to store sealed sources containing plutonium-239, strontium-90, and cesium-137, and develop a plan to ensure the continued recovery of greater-than-Class-C waste until a disposal facility is available.** Highlights: <http://www.gao.gov/highlights/d03483high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-03-483>

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

Chemical Sector

5. *May 13, Associated Press* — A bad year expected for Louisiana's chemical industry .

Louisiana's chemical industry is in for a rocky year as energy prices remain high and manufacturing jobs go overseas, a leading state economist said. **Louisiana State University's Loren Scott predicts that the industry will lose more than 2,000 jobs in the next two years and he warned that the cuts could be permanent.** "The industry is really suffering through an extended downturn," said Ken Stern, national industry director for chemicals at accounting firm KPMG in New York **High energy prices are to blame but so is growing competition from overseas plants, many of which are owned by chemical makers with U.S. operations. The state's chemical makers compete with plants in nations where natural gas is so cheap that excess capacity is burned off.** The United States last year lost its longtime standing as a net exporter of chemicals as shipments from Western Europe and Asia reversed the trade balance. The balance slipped from a \$1.3 billion U.S. surplus in 2001 to last year's deficit of \$4.4 billion. In the mid-1980s, one in four chemical jobs disappeared in Louisiana when a strong dollar made foreign products cheaper than U.S.-produced chemicals.

Source: <http://www.theadvertiser.com/business/html/B9CC567A-4CA0-4BA8-B207-00EE19B436AB.shtml>

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

Defense Industrial Base Sector

6. *May 13, Government Executive* — Defense contractors get into homeland security business.

Large, traditional defense contractors have easily remade themselves to be homeland security providers since the September 2001 terrorist attacks. But none appear to have made drastic changes that would redefine their core businesses. **For years, the industry has been providing to the Defense Department and the intelligence community physical and cyber security services that can be used for domestic security, such as protection of networks, interoperability and network-centric operations.** One reason for not completely redefining a company might be that the homeland security funding has not yet begun to flow like Defense or intelligence money does. Almost all of Homeland Security's fiscal 2003 budget of nearly \$38 billion has gone toward personnel and operations, not procurement.

Source: <http://www.govexec.com/dailyfed/0503/051203td1.htm>

7. *May 08, U.S. Department of Defense* — **'Guardian' project to bolster force, installation security.** A new DoD force and installation security project targeted against terrorist threats – to include possible use of weapons of mass destruction — is slated to debut October 1. **The \$1 billion effort, named "Guardian," will ultimately bolster anti-terrorism force protection and security at about 200 stateside installations and overseas posts over the next five years,** Army Brig. Gen. Stephen Reeves, DoD's program executive officer for chemical and biological defense, said in an interview May 6. **"Guardian," according to Reeves, will provide affected military facilities and their populations with enhanced protection against "chemical, biological, radiological and nuclear threats."** The project will also "integrate that (new) protection capability with the existing force protection measures that are on that installation," he pointed out. "Guardian," Reeves continued, "is really there to assist commanders in providing force protection for (U.S. military) installations around the world." Source: http://www.defenselink.mil/news/May2003/n05082003_200305084.html

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

Banking and Finance Sector

8. *May 13, U.S. Department of the Treasury* — **Secretary Snow remarks upon unveiling of new twenty dollar bill.** The purpose of the new design is to stay ahead of anyone who would compromise the security and integrity of the dollar through counterfeiting. Thanks to the changes we made to our currency in the late 1990s, aggressive law enforcement efforts led by the Secret Service, and the help of an informed public, we've been able to do just that. Nonetheless, technology changes quickly and counterfeiters develop new tools, so we plan to introduce new designs for our currency every 7 to 10 years. In fact, as soon as the current \$20 note was introduced in 1998, work began on the new design you're about to see. **This new \$20 note will go into circulation later this year. New designs for the \$50 and \$100 notes will follow in 2004 and 2005. The most distinctive change in the new currency design is the color. Different colors for different denominations will make it easier to tell one note from another, especially for those with visual impairments. Color also makes the currency more difficult to counterfeit.** Source: <http://www.treasury.gov/press/releases/js369.htm>

9. *May 13, Dow Jones Newswires* — **SEC accuses man of internet fraud.** The lawsuit by the Securities and Exchange Commission, filed in Federal District Court in Tennessee, charged K. C. Smith with raising \$102,554 through bogus Web sites and about nine million unsolicited e-mail messages. Smith used the S.E.C. seal to convince investors the scheme was legitimate, according to the suit. **Smith of Oak Grove, KY, did not admit to nor deny the accusations, but agreed to a settlement requiring him to return \$107,510 of gains and interest, and barring him from future violations. Regulators said that from May 2002 to February 2003, Smith ran a Web site for Kryer Financial, a bogus investment company offering double-digit monthly returns said to be insured by the "United States Deposit Insurance Corporation," another entity he invented.** Source: <http://www.nytimes.com/2003/05/13/technology/13SEC.html>

10. *May 09, U.S. Attorneys Office, Camden, New Jersey* — **Nine indicted, seven arrested in nationwide \$10 million money order scam.** Seven suspects were arrested in early morning

raids on Friday, May 9, taking the main players in an organization that produced well over \$10 million worth of fictitious money orders that appeared to be issued by the federal government, U.S. Attorney Christopher J. Christie announced. **A 25-count Indictment unsealed with today's arrests describes an elaborate fraud by a group of individuals working in the Camden and Atlantic City area who produced false money orders and submitted them as payment for mortgages, auto loans, and other personal items, such as tickets aboard the Concorde supersonic jet. As the Indictment alleges, they regularly met to discuss the fraudulent scheme and ways to avoid law enforcement detection.** The Indictment puts the fraud at \$10 million, but Christie said, the total face value of the fraudulent money orders exceeds \$50 million.

Source: http://www.njusao.org/files/ha0509_r.htm

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

Transportation Sector

11. *May 13, New York Times* — **Smaller U.S. airports are increasingly popular. A growing number of business travelers shunning the larger, more congested airports and are flying out of smaller regional airports instead, thereby not only sparing themselves a lot of aggravation, but saving money as well.** Low-cost airlines like Southwest prefer these smaller fields precisely because they are less congested, and because they charge lower landing fees. The shift of business travel to regional airports is illustrated by Federal Aviation Administration statistics. They show big gains in passenger traffic at airports just outside some major urban areas from 1996 to 2001 — the latest year for which statistics are available — while the traffic at primary airports grew little or actually shrank. **The gains at these suburban airports came even as the weak economy led many airlines to cut service to midsize and small cities. "In an effort to stem losses, airlines have reduced service in the smallest communities by 19 percent in the past five years,"** Kenneth M. Mead, the inspector general of the Department of Transportation, testified before a Senate subcommittee earlier this month.

Source: <http://www.nytimes.com/2003/05/13/business/13SMAL.html>

12. *May 13, Federal Computer Week* — **DHS seeks more dollars for border technology.** The Homeland Security Department (DHS) told congressional appropriators on Tuesday that more money is needed in fiscal 2004 for high-tech devices and solutions to tighten U.S. seaports, airports and on land borders. Robert Bonner, commissioner of the Bureau of Customs and Border Protection, which is part of DHS, said the White House is seeking \$338.2 million for the bureau to prevent terrorists and their weapons from entering the United States. **The money would be used to continue funding programs such as the Container Security Initiative, which involves inspecting cargo before it leaves a foreign port, as well as deploying new technologies to detect conventional explosives and weapons of mass destruction.** "These funds will continue to support the automation and information technology programs that will improve overall operations of the agency, and the traditional missions for which the [agency] is responsible," Bonner told the Senate Appropriations Committee's Homeland Security Subcommittee.

Source: <http://www.fcw.com/fcw/articles/2003/0512/web-border-05-13-03.asp>

13.

May 12, Federal Computer Week — **Smart cameras to watch Canadian borders.** The U.S. Bureau of Customs and Border Protection is stepping up security on the border with Canada by **deploying intelligent software for hundreds of video cameras that can see and analyze unusual activities or movements in real time. This is part of a larger project to use state-of-the-art technology to tighten border control in the wake of the September 11, 2001, terrorist attacks.** The software allows users to program the system to look for specific objects or any activity out of the ordinary — a person climbing a fence, for example, or an unusual object at the border. It's surveillance by exception. The system sifts through the vast majority of routine images, so users can focus on causes for concern. **The software evaluates surveillance videos as they are captured, so the bureau can respond immediately if something suspicious is found.** The technology uses artificial intelligence known as computer vision to detect and identify objects captured on video. It enables bureau officials to use manpower more efficiently. Instead of relying on an individual to monitor a computer screen, the software does it for the agency.

Source: <http://www.fcw.com/fcw/articles/2003/0512/news-cameras-05-12-03.asp>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

14. *May 13, BBC News* — **German bird flu confirmed. Germany has confirmed that it has uncovered its first case of the highly contagious bird flu that has ravaged farms in Belgium and the Netherlands.** The health ministry said that tests on a farm in Viersen, near the Dutch border in western Germany, were positive. The confirmation comes four days after veterinary officials slaughtered 32,000 chickens to try to contain the disease. Farmers within one kilometre of Viersen had been ordered to slaughter poultry as a precaution, roads were sealed off and disinfection points set up. **The European Commission has extended to Germany emergency measures already imposed on Belgium and the Netherlands.**

Source: <http://news.bbc.co.uk/1/hi/world/europe/3024509.stm>

15. *May 13, Agriculture Online* — **U.S. takes EU biotech ban to WTO. The U.S., Argentina, Canada, and Egypt will file a World Trade Organization (WTO) case against the European Union (EU) over its five-year moratorium on approving agricultural biotech products U.S. Trade Representative Robert Zoellick and Agriculture Secretary Ann Veneman announced today. At least nine other countries have expressed support and joined the case as third parties.** But EU officials maintain the ban is less about trade and more about giving consumers the assurances they want about food safety. "The EU's moratorium violates WTO rules," said Zoellick. "We've waited patiently for five years for the EU to follow the WTO rules and the recommendations of the European Commission (EC), so as to respect safety findings based on careful science. "The EU's persistent resistance to abiding by its WTO obligations has perpetuated a trade barrier unwarranted by the EC's own scientific analysis,

which impedes the global use of a technology that could be of great benefit to farmers and consumers around the world," said Zoellick.

Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=MonsentoDetail_ANewsindex_html_49895

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

Food Sector

16. *May 08, Food and Drug Administration* — **HHS announces new funding opportunity for state food labs. The Food and Drug Administration (FDA) and the U.S. Centers for Disease Control (CDC) are working to expand the National Laboratory Response Network (LRN) and the Food Emergency Response Network (FERN) to include a substantial number of counter terrorism laboratories capable of analyzing foods.** The CDC is expanding the scope of its cooperative agreements in the current funding cycle to include preparedness and response capacity of state food laboratories and other laboratories. **The expanded network will accommodate the need for effective and efficient testing of food specimens to help public health officials deal with apparent or actual incidents of biological or chemical terrorism.** This broader network is imperative because, during a terrorist event that involves food, public health laboratories that analyze clinical specimens will be busy with their primary work. Analyzing food requires special equipment, reagents, and skills.

Source: <http://www.fda.gov/oc/bioterrorism/foodlab.html>

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

Water Sector

17. *May 12, Associated Press* — **Park City considers punishing water violators. Park City, UT officials are considering an ordinance that would provide stiff fines and possible jail sentences for breaking water-conservation regulations.** Depending on drought severity, violation of the watering law could be a class B misdemeanor, punishable by up to six months in jail and a \$1,000 fines. Other possible punishments would include city-enforced fines of \$50 to \$500 a day or having water service turned off. If the proposal passes, Park City will become one of a very limited number of Utah cities that make violation of water conservation laws a criminal misdemeanor.

Source: <http://tv.ksl.com/index.php?nid=5ont>>

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

Public Health Sector

18. *May 13, United Press International* — **Cold drug could yield SARS treatment. A drug currently being tested in humans — prevent the common cold could lead to treatments for Severe Acute Respiratory Syndrome (SARS), a study released Tuesday suggests.** So far, scientists have not yet identified an effective medication against the SARS virus, which has

spread quickly around the world infecting more than 7,000 people and causing more than 500 deaths. But the new study gives hope an effective treatment could be developed. Researchers conducted molecular analysis of the SARS virus and found a drug called AG7708, which is being developed to treat the common cold, "might be a good starting point for the development of drugs against" the organism, the study's principal investigator, Rolf Hilgenfeld of the University of Luebeck, Germany, said during a teleconference from Germany. **In the study, Hilgenfeld's group found a protein expressed by the SARS virus is very similar to a protein expressed by the rhinovirus, which causes the common cold. Because the protein is an enzyme called protease, which is essential to the replication cycle of the virus, blocking the protease should keep the virus from making copies of itself and thereby prevent the breathing problems and death seen in some SARS patients.**

Source: <http://www.upi.com/view.cfm?StoryID=20030513-123814-9178r>

19. *May 12, New York Times* — **New weapon in arsenal against chemical attack.** In the hunt for terrorists who might try to use unconventional weapons on American soil, the federal government is enlisting an old, and very trusted, ally. **The Department of Homeland Security says that in a research program kept quiet for months, it has determined, apparently for the first time, that ordinary dogs can be trained to sniff out trace amounts of the nonlethal components of chemical weapons, including sarin and cyanide. As a result, the department's Bureau of Customs and Border Protection has begun to train a corps of chemical detector dogs and is planning to deploy them at airports, seaports, government buildings, and other potential terrorist targets, where they will work alongside the police dogs that have long been used to sniff out narcotics, explosives, and human remains.** So far, several dogs, the department will not give an exact number, saying that to do so would tip off terrorists to the scope of the program, have been given chemical training. Hundreds more are expected to be added to the program in the next two years. The discovery that dogs can apparently detect components of chemical weapons has implications beyond national security. Officials hope it will also mean budget savings for the federal government, which now spends hundreds of millions of dollars a year on research to develop machinery to detect chemical weapons.

Source: <http://www.nytimes.com/2003/05/13/international/worldspecial /13HOME.html>

20. *May 12, Associated Press* — **SARS strains U.S. health system.** Keeping Severe Acute Respiratory Syndrome (SARS) from spreading in the U.S. is straining the public health system. **Health departments that already were struggling to deal with bioterrorism and West Nile virus say their ability to protect against more common threats today is compromised. "Critically important things are not being done," says Dr. Alonzo Plough, public health director for Seattle–King County, WA. The U.S. Centers for Disease Control and Prevention (CDC) is stretched, too, despite an emergency \$16 million from Congress to fight SARS.** What if the anticipated summer resurgence of West Nile virus occurs at the same time as some other outbreak, perhaps food poisoning, and SARS is still around? Could CDC possibly handle it all, wonders Barry Bloom, dean of Harvard's School of Public Health. And Dr. Georges Benjamin, head of the American Public Health Association, says, "Every crisis du jour forces tradeoffs, attention to one infectious disease at the expense of another." Benjamin told members of Congress they play "a public health shell game" by funding CDC to handle one headline-grabbing problem at a time instead of paying for a seamless system that tackles everyday illnesses with a built-in capacity for emergencies.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A46806-2003May 12.html>

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

Government Sector

21. *May 13, Boston Herald* — Feds to help defray Hub convention security costs.

Cash-strapped planners of next year's Democratic National Convention got a helping hand from Uncle Sam yesterday as federal officials promised to help defray skyrocketing security costs for the presidential nominating party. **Designating the event a national special security event in the wake of the Sept. 11, 2001, terrorist attacks, the U.S. Department of Homeland Security gave security control to the Secret Service. Doing so could significantly cut the expected \$10 million security costs and gives the Secret Service the top job in keeping 35,000 convention-goers and the public safe – not local cops.**

Source: http://www2.bostonherald.com/news/local_regional/conv05132003.htm

22. *May 13, New York Times* — U.S. to rely more on private companies' satellite images.

President Bush is ordering federal agencies to rely much more heavily on private satellite companies to provide images from space, a significant shift from current policy, administration officials said on Monday. **The new policy seeks to limit the government's own network of satellites to the most sensitive, high-priority assignments and use private vendors to meet relatively routine tasks "to the maximum practical extent," officials said. The shift is seen as an effort both to bolster the position of American satellite companies in the global marketplace and, in the long term, to save money.** The White House is expected to announce the new policy on Tuesday after a review that began late last year.

Source: <http://www.nytimes.com/2003/05/13/national/13SATE.html>

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

Emergency Services Sector

23. *May 13, Washington Times* — FBI lists deaths of officers in 2002. A total of 56

law-enforcement officers nationwide were slain in the line of duty during 2002, according to preliminary statistics released yesterday by the FBI's Uniform Crime Reporting (UCR) program. Another 76 officers were accidentally killed on duty last year, the FBI said. The UCR report states that of the 56 deliberate killings, 25 were in the South, 12 in the Midwest, nine in the West and five in the Northeast. Another five officers also were killed in Puerto Rico.

Source: <http://www.washingtontimes.com/national/20030513-32522300.htm>

24. *May 13, Government Computer News* — Web portal is communications hub for terrorist drill. Government emergency response workers this week are using a Web portal to exchange vital information during TOPOFF2, the national terrorist attack exercise in Chicago, Seattle and Washington. The five-day exercise includes a simulated radioactive dirty bomb attack on Seattle and a biological attack on Chicago. It's the second such drill the federal government has overseen; the first was held prior to the terrorist attacks in 2001. **The portal is intended to help overcome traditional stovepipe barriers to collaboration across levels of government,**

Topoff2 officials said. "This is a password-protected, Web-based architecture that allows all the important responders to participate and get the data they need to do their jobs," Topoff2 co-director Theodore Macklin, a member of Homeland Security's Office for Domestic Preparedness, said on Monday.

Source: http://www.gcn.com/vol1_no1/daily-updates/22040-1.html

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

Information and Telecommunications Sector

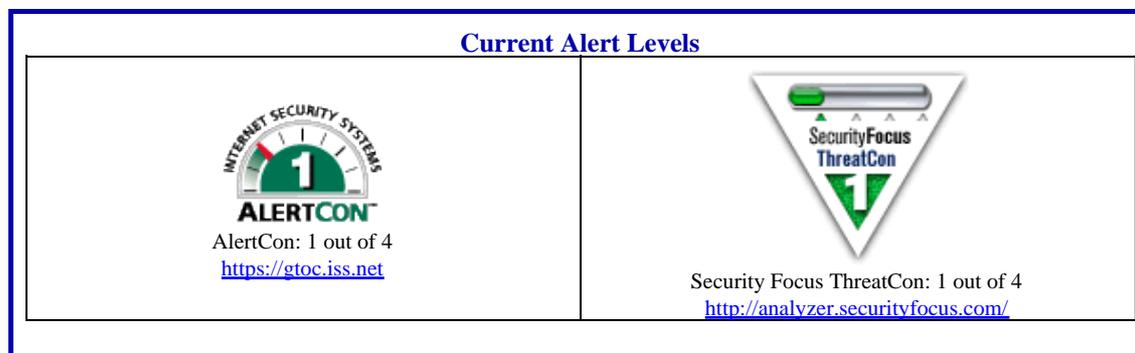
25. *May 12, The Register* — **Fizzer stealth worm spreads via KaZaA.** An Internet worm called "Fizzer" is spreading through the KaZaA P2P file-sharing network and as an executable file via e-mail. Reuters reported Monday that **businesses in Asia were the first to report the attack, followed by reports of tens of thousands of infections in Europe. Fizzer is especially dangerous because it installs a keyboard-logging program** that intercepts and records all keyboard strokes in a separate log file. **To transmit this information, Fizzer loads a backdoor utility** that allows crackers/VXers to control a computer via IRC channels. Additionally, **the worm regularly connects with Web page located on the Geocities server from which it attempts to download updated version of its executable modules.** In an attempt to foil detection, **Fizzer also attempts to shut down an array of widely used anti-virus programs that might be running on a victim's PC.** Computer users should keep their anti-virus software updated.

Source: <http://www.theregister.co.uk/content/56/30659.html>

26. *May 12, National Journal* — **Report to recognize agencies' progress toward IT security.** President Bush's administration is readying a report that will recognize several government agencies for making tangible progress in their efforts to meet security goals for information technology, according to administration officials. **The White House Office of Management and Budget (OMB) is preparing to send Congress an annual report highlighting the status of those IT initiatives,** OMB analysts told members of a National Institute of Standards and Technology advisory board last Wednesday. The report will be the last IT security review by OMB before it updates its guidelines and agency reporting requirements under new IT rules created under a recent e-government law.

Source: <http://www.govexec.com/dailyfed/0303/031203td2.htm>

Internet Alert Dashboard



Current Virus and Port Attacks

Virus:	#1 Virus in the United States: WORM_LOVGATE.F Source: http://wtc.trendmicro.com/wtc/wmap.html ; Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	80 (www), 137 (netbios-ns), 1434 (ms-sql-m), 25 (smtp), 113 (ident), 445 (microsoft-ds), 4662 (eDonkey2000), 139 (netbios-ssn), 0 (----), 3 (compressnet) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

27. *May 13, Associated Press* — **Terror sleeper cell suspect pleads guilty.** A fifth member of an alleged terrorist sleeper cell in a Buffalo suburb pleaded guilty on Monday to supporting terrorism. **Yasein Taher, 25, admitted learning to fire guns and grenade launchers at an al Qaeda camp in Afghanistan months before the September 11, 2001, attacks. Taher, acting against his attorney's advice, became the fifth member of a group of six Yemeni Americans to enter a plea agreement with the government in the case. He is expected to receive an eight-year prison term when he is sentenced in September.** Prosecutors said Taher trained at the Afghan camp and was a member of a sleeper cell, a team of trained terrorists who lie dormant until called to action. The other men, Faysal Galab, 27; Shafal Mosed, 24; Sahim Alwan, 30; and Yahya Goba, 26, also have been offered sentences of between seven and 10 years. The sentences are contingent upon their cooperation in this and future terrorism investigations.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A47262-2003May 12.html>

28. *May 13, Associated Press* — **Philippine ultimatum for Muslim rebels.** The government threatened Tuesday to declare a Muslim rebel group a terrorist organization unless it stops attacking civilians and takes tangible steps toward ending violence in the southern Philippines within two weeks. **The Moro Islamic Liberation Front, blamed for a bomb attack that killed 10 people Saturday, has until June 1 to renounce terrorism and turn over members responsible for recent attacks on civilians, presidential spokesman Ignacio Bunye said. Otherwise, the government will declare the MILF a terrorist organization and ask the United States to include the group on its own terrorist list, Bunye said. A U.S. listing imposes financial and visa penalties on group members.** The Philippine government has been reluctant to put a terrorist tag on the MILF, who have been fighting for a separate Muslim homeland, for fear it may disrupt sporadic peace talks with the rebels.

Source: <http://www.cbsnews.com/stories/2003/05/13/attack/main553659.shtml>

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

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.