Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 05 May 2005

Current Nationwide Threat Level is
[fetch threat level]
[set manually]
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports a Canadian customs union official says a fatal shooting in northwestern Montana, just a short distance from a U.S.−Canada border crossing, has highlighted confusion surrounding security along the world's longest unarmed border. (See item 10)
- The Daily Local reports officials from the Department of Emergency Services in Chester County, PA, have been organizing classes in awareness training on weapons of mass destruction for police and ambulance workers. (See item 23)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact 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 04, Sun−Sentinel (FL)* — **New nuclear power plants proposed by Nuclear Regulatory Commission chairman.** The United States needs to add about 100 nuclear power plants over the next two decades to meet burgeoning demand for electric power and maintain the current generating mix, said Nils J. Diaz, chairman of the Nuclear Regulatory Commission (NRC), on Tuesday, May 3. Nuclear power currently accounts for 20 percent of electric energy generated in the country, while fossil fuels and hydroelectric power produce most of the remainder. Diaz said that the federal government has taken a series of steps to encourage private companies to build and expand nuclear facilities, while at the same time upgrading plant security norms.

These include simplifying the complex licensing procedures and encouraging development of standardized plant designs. Diaz said that building or expanding nuclear plants on existing sites would cut down on overall planning and construction costs and expedite the permitting process. The commission expects five or six new applications for plants over the next several years and will seek additional funding so that it will have adequate technical staff to handle them. Source: http://www.sun−sentinel.com/business/local/sfl−zfpl04may04,0 ,1142996.story?coll=sfla−business−headlines

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *May 04, Associated Press* — **Water plant chlorine leak leads to evacuations.** A chlorine leak at the city water plant in Thibodaux, LA, forced the evacuation of most of downtown for several hours Wednesday, May 4. Lafourche Parish authorities said there were no reports of serious injuries. Dan Naquin, assistant chief of the Thibodaux Fire Department, said a worker was transferring chlorine from one tank to another when a valve broke and the chemical escaped. Authorities said about 500 pounds of chlorine was in the 1−ton cylinder but they did not know how much escaped. Hazardous−materials crews were responded to the spill. Chlorine is used to kill bacteria and other microbes in drinking water. When undiluted, it produces strong fumes that can cause coughing and chest pain or water retention in the lungs. It irritates the skin, the eyes and the respiratory system. Director of public works, Kermit Kramer, said two workers were treated and released from a hospital and were back at work by Wednesday afternoon. The evacuation zone also included City Hall and the headquarters of the city library. Source: http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/2005 0504/APN/505040798

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *May 04, Turnto10.com (RI)* — **E−mailed surveys may involve phishing.** Phishing scams involving bank surveys are duping online users. A victim recently fell for an e−mail purporting to be from Citizen Bank that invited her to participate in a customer service survey. For her trouble, $5 would be deposited into her account. However, the e−mail wasn't from Citizens Bank. The scammers hijacked the bank's logo, tricked the victim into giving up her account number and PIN, and cleaned out her bank account. The U.S. Secret Service is one of the agencies in charge of investigating Internet financial crimes. However, the problem is, many of the perpetrators are overseas. "They could be in Cranston (RI) or they could be in Romania," said Thomas Powers, of the Providence Secret Service office. Powers said even when foreign governments cooperate; technology often allows the scammers to stay a step ahead. "Instead of being in streets or in banks, they're in apartment buildings or in homes, hiding behind

computers," said Powers. "So they're really −− they're really covert," said Powers.
Source: http://www.turnto10.com/money/4445620/detail.html

4. *May 04, The New Zealand Herald* — **Suspect package at bank building destroyed by bomb squad.** A suspicious package found at the Citibank building in downtown Auckland, New Zealand, was destroyed on Wednesday, May 4, by bomb disposal experts. Police said the package, a briefcase, did not contain a bomb or other explosive device. The package was found about 10 a.m. on an outside first−floor balcony by a person who worked in the multi−storey Citibank building, which also houses the U.S. Consulate, said police communications manager Noreen Hegarty.
Source: http://www.nzherald.co.nz/index.cfm?c_id=1&ObjectID=10123819

5. *May 04, The Gazette (Canada)* — **Identity theft is top problem according to executive.** The biggest computer security issues facing consumers and businesses today are identity and information theft, says a top executive at leading computer security firm McAfee Inc. As an ever−increasing number of new viruses, worms, spyware and adware are discovered every day, it is crucial to consistently and regularly protect computer systems against unauthorized intrusions, experts say. During a meeting with journalists, McAfee chief security officer Ted Barlow said hackers are no longer interested in breaking into computer systems and causing them to crash. Instead, they now want to keep a system up and running so they can steal information from it or use it as a launching pad for attacks against other computers.
Source: http://www.canada.com/technology/story.html?id=d4a55ba3−85e3−4399−847c−dddc35af62c3

6. *May 04, Netcraft* — **Scammers deploy botnets to sustain phishing attacks.** Botnets controlled by scammers are running their own Domain Name System (DNS) nameservers on compromised computers, complicating the task of shutting down malicious sites. The technique can keep phishing sites accessible longer by making the nameservers a widely distributed moving target amongst thousands of compromised machines within a bot network. The sophisticated new strategy makes it harder to target phishing sites at the nameserver level, which can be the most effective route to taking a malicious site offline. If scammers are able to compete effectively by deploying botnets as nameservers, additional emphasis will be placed upon the responsiveness of domain registrars. Bot networks aggregate computers that have been compromised allowing them to be remotely directed by the attackers. Botnets are being used for a variety of scams, including spamming, phishing, sniffing network traffic for unencrypted passwords, and click fraud targeting Google's AdSense program. A March report found that at least one million compromised machines are being used in botnets.
Source: http://news.netcraft.com/archives/2005/05/04/fraudsters_deploy_botnets_as_dns_servers_to_sustain_phishing_attacks.html

[Return to top]

Transportation and Border Security Sector

7. *May 04, Government Accountability Office* — **GAO−05−657T: Airport and Airway Trust Fund: Preliminary Observations on Past, Present, and Future (Testimony).** The Airport

and Airway Trust Fund (Trust Fund) was established in 1970 to help fund the development of a nationwide airport and airway system and to fund investments in air traffic control facilities. It provides all of the funding for the Federal Aviation Administration's (FAA) accounts such as the Airport Improvement Program (AIP), which provides grants for construction and safety projects at airports, the Facilities and Equipment (F&E), which funds technological improvements to the air traffic control system, and the Research, Engineering, and Development (RE&D). In addition, the Trust Fund provides some funding for FAA's operations account. To fund these accounts, the Trust Fund relies on a number of taxes for revenue, including passenger ticket, fuel, and cargo taxes that are paid by passengers and airlines. Since 1970, revenues have generally exceeded expenditures −− resulting in a surplus or an uncommitted balance. In 2004, the Trust Fund's year end uncommitted balance was about $2 billion. A number of structural changes in the aviation industry and external events have affected revenues flowing into and out of the Fund and have caused some aviation stakeholders to speculate about the Fund's financial condition. The various taxes that accrue to the Trust Fund are scheduled to expire in 2007. The Government Accountability Office was asked to provide information and analysis about the financial outlook of the Trust Fund.
Highlights: http://www.gao.gov/highlights/d05657thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−657T

8. *May 04, Associated Press* — **Airline passengers to be asked for more data.** Airline passengers soon will be asked to provide their full names and birth dates when they buy tickets. In coming weeks, the Transportation Security Administration (TSA) plans to require airlines to solicit the information. Passengers do not have to provide it, though if they don't there's a better chance they'll have to undergo more stringent screening at the airport, Justin Oberman, the TSA official in charge of the program, said Wednesday, May 4. Oberman said having passengers' full names and birth dates will make it less likely that they'll be confused with people who are known or suspected terrorists. The request for extra information is part of the TSA's effort to build a new computerized passenger screening program, called Secure Flight, which would allow the TSA to take over from the airlines the responsibility of checking passengers' names against the watch lists. The TSA plans to begin Secure Flight with two airlines in August.
Source: http://news.yahoo.com/s/ap/20050504/ap_on_re_us/passenger_screening;_ylt=A86.I07gD3lCRiEBgwSs0NUE;_ylu=X3oDMTA2M2YzbmJmBHNlYwN1cw−−

9. *May 04, Canadian Press* — **Package sparks scare at Quebec airport.** A tiny package caused a big scare at Montreal's main airport late Tuesday, May 3, scrambling emergency crews and sending one man to hospital. Four people complained of feeling ill from a nauseating smell coming from a tiny package about the size of a ring box and containing an unidentified white powder when it passed through customs. "There was no link with the substance that was found," said Eric Berry, a spokesperson for Urgences sante, the citywide ambulance service. He suggested stress from the incident may have been a factor. "When it arrived at Canadian customs, an employee opened the package and saw the substance inside," Montreal police Const. Miguel Alston said. When the employee reported feeling ill, emergency crews were called. The owner of the package wasn't with it and police are not sure if the owner was on the flight. An investigation is continuing. The substance was sent to a provincial public health laboratory for analysis.
Source: http://www.canada.com/fortstjohn/story.html?id=c2f82a09−5150

−462b−aca0−fd3ab3d1759d

10. *May 04, Associated Press* — **Border shooting highlights confusion over security.** A Canadian customs union official says a fatal shooting in northwestern Montana, just a short distance from a U.S.−Canada border crossing, has highlighted confusion surrounding security along the world's longest unarmed border. Sheriff deputies from Montana's Lincoln County were dispatched to the Roosville border crossing between British Columbia and Montana after reports of gunfire on Saturday, April 30. Robert Donald Mast, 42, of Eureka, was found dead several feet from the Canadian border in the United States. Eureka, MT, police later arrested Wayne Allen Hixon, 51, also of Eureka, who was coming from the border area. On the northern side of the border, Canadian customs officials called the nearby Royal Canadian Mounted Police for assistance when the shooting broke out, said Ron Moran of the Customs Excise Union Douanes Accise, the union representing Canadian customs officers. "There is nobody on the Canadian side patrolling the Canadian border," he said, adding that the job nominally falls to the Mounties. Moran said the situation along the 4,000−mile border has become a "bureaucratic football." The U.S. side of the border is monitored by armed agents, though far fewer than are posted along the Mexican border.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2005/05/04/build/state/35−bordershooting.inc

11. *May 04, North Jersey Media Group* — **Plan to boost ports' freight rail capacity is ahead of schedule.** With record cargo volume flowing through its ports, the Port Authority of New York and New Jersey on Wednesday, May 4, moved up a planned expansion of the ports' freight rail capacity. Agency officials touted the expedited projects at Port Newark and Port Elizabeth−Port Authority Marine Terminal as critical steps in keeping up with demand and cutting into the growing truck traffic clogging New Jersey roads. Six more miles of support track, eight new loading tracks and a new support center could be finished as much as two years earlier than originally planned, agency officials said after authorizing $141 million for the projects. The action comes a month after officials touted a record 4.4 million containers handled at the ports last year, up more than 10 percent from 2003. Port Authority officials have been working on a $600 million plan to expand rail operations at the ports.
Source: http://www.manufacturing.net/lm/index.asp?layout=articleXml& xmlId=276038658

12. *May 04, Associated Press* — **Suspicious package prompts partial evacuation of Bradley terminal.** A terminal at Bradley International Airport, in Windsor Locks, CT, was partially evacuated early Wednesday, May 4, because of a suspicious package that turned out to be machine parts. State police said the package was being screened before it was delivered to one of the airlines when it was flagged as a possible explosive device. The state police bomb squad and the Transportation Safety Administration determined the package was not dangerous. The scanner "did its job," said John Wallace, a spokesperson for the airport. "It set of the alert and we took all necessary precautions for everybody's safety."
Source: http://www.stamfordadvocate.com/news/local/state/hc−04140920.apds.m0554.bc−ct−brf−−may04,0,2151071.story?coll=hc−headlin es−local−wire

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *May 04, Marshfield News−Herald (WI)* — **Wisconsin county leader in agriterror response.** Scenario: the dairy cows have lost their appetite, dropped milk production, have blistering tongues, and are running a fever without explanation. They continue to worsen over the next week, prompting a farm−wide search. Only then, the farmer finds the broken bottles near the fence. Foot−and−mouth disease is spreading through the herd. That scenario, while hypothetical, was discussed in September when officials in Clark County, WI, met to discuss their planned reaction to an agriterrorism attack. September's tabletop exercise brought together various agencies in an effort to develop a working picture through the process. Since an act of terrorism falls under federal jurisdiction, much of the planning deals with the logistics of providing facilities for incoming officials. Clark County would have a difficult time with large numbers of people. That's why county officials are planning now, rather than compounding the problem later with a confused reaction, Matt Jorgensen, dairy and livestock agent for Clark County's University of Wisconsin−Extension, said. To help control the rush of reality, officials are planning a series of fictional trials. An exercise design team will be established over the summer in preparation for a "functional exercise" in September, one step short of a full−scale exercise which officials are hoping for in 2006.
    Source: http://www.wisinfo.com/newsherald/mnhlocal/285278930285547.s html

14. *May 04, USAgNet* — **Pioneer helps farmers track the spread of soy rust.** To help track the spread of Asian soybean rust, Pioneer Hi−Bred International, Inc., is working with the U.S. Department of Agriculture (USDA) to track confirmed cases of rust, as identified by Pioneer agronomists and archived in the Pioneer Field Information eXchange (PFIX) system. "With nearly 200 agronomists using the PFIX system, the information gathered will be invaluable in tracking the spread of the disease and helping growers prepare for its potential arrival in their soybean fields," said Tom Hall, Pioneer technical applications manager. The PFIX system was designed to capture field observations using a Personal Digital Assistant (PDA) handheld computer. Agronomists input information collected during service calls and create a geo−referenced archive of observations. In the last two years, PFIX has helped Pioneer agronomists monitor the movement of many insects and pests, including soybean aphids in 2003. This will be the first time the information will be shared publicly with growers.
    Pioneer maps tracking the spread of rust: http://www.pioneer.com/growingpoint
    Source: http://www.usagnet.com/story−national.cfm?Id=464&yr=2005

15. *May 04, Cambridge Evening News (United Kingdom)* — **Genome sequence helps fight illness.** Scientists in Cambridge, England, have come a step closer to combating chlamydial disease. Researchers at the Wellcome Trust Sanger Institute in Hinxton have published the genome sequence of Chlamydophila abortus, a major pathogen of domestic animals. Chlamydophila abortus is the most common cause of infectious abortion in sheep in the United Kingdom. The genome sequence will bring new possibilities in the fight to control the spread of infection.
    Source: http://www.cambridge−news.co.uk/news/city/2005/05/04/a9056ab

b−fd2c−46dd−98a5−917ed244c4a1.lpf

16. *May 04, Associated Press* — **Beetle damaging saplings in Arkansas.** Scientists say a beetle that first appeared in Arkansas about three years ago is killing saplings in the central part of the state and beyond. The Asian Ambrosia Beetle is devouring the bark of woody ornamental, fruit, and nut trees. The beetle also attacks red maples, Japanese maples, pecan, and peach trees that are less than five years old. The insect, which arrived in the U.S. in 1974 at a port in Charleston, SC, bores its way through the trunk of the saplings. The damage can introduce pathogenic fungi that prove lethal to the trees. The beetle feeds on the fungi and the female lays her eggs in the tree. Because the beetle can't be eliminated by insecticides once it has burrowed through the bark, chemicals have proven ineffective. So, too, are fungicides.
Source: http://abcnews.go.com/Technology/wireStory?id=726935

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

17. *May 03, Associated Press* — **Malaria kills one million a year.** Malaria kills more than one million people and sickens between 350 million and 500 million people a year, mainly in Africa, according to a report released Tuesday, May 3. The report, released by the World Health Organization and UNICEF, is the first comprehensive report on malaria worldwide. Nine out of 10 malaria deaths are among sub−Saharan African children under the age of 5. About 40 percent of the world's population is at risk from malaria, a parasitic, mosquito−borne disease. The regions hardest hit after Africa are Southeast Asia, the eastern Mediterranean region, and the Western Pacific. In many parts of Africa and most of Asia, malaria has become more resistant to traditional treatments.
World Malaria report: http://rbm.who.int/wmr2005/
Source: http://www.sci−tech−today.com/story.xhtml?story_id=34115

18. *May 03, Associated Press* — **Military to resume voluntary anthrax shots.** The military will resume giving the anthrax vaccine to volunteers as soon as this week, Pentagon officials said Tuesday, May 3. During the next six months, the vaccine will be primarily given to troops who are serving in Korea, the Middle East, and South Asia, the Pentagon said. It will also go to soldiers who work in counterterrorism roles related to defense against biological weapons inside the U.S. They will be informed of the benefits and risks of the vaccine and will be allowed to opt out without penalty, the Pentagon said. The military had been prohibited from

giving vaccine shots to the troops since October 2004, when a judge found fault in the Food and Drug Administration's process for approving the drug. In April, U.S. District Court Judge Emmet Sullivan said the military could begin giving the vaccine on a voluntary basis under a new law allowing for the emergency use of unapproved drugs. The Pentagon contends the possibility of anthrax on the battlefield and terrorist attacks constitutes an emergency. The Defense Department will continue to press for mandatory vaccine shots, said Perry Bishop, a health affairs spokesperson for the Pentagon. The military can only administer the vaccine for six months as an emergency measure, officials said.
Source: http://news.yahoo.com/s/ap/20050503/ap_on_he_me/military_anthrax;_ylt=Ak3qizrk554avOf9HLxMvM5Z24cA;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

19. *May 03, World Health Organization* — **World Health Organization to go online to combat fake drugs business.** The World Health Organization (WHO) will harness the power of the Internet in its war on counterfeit drugs. At a workshop in Manila, Philippines, from May 4 through 6, the WHO will unveil its Rapid Alert System (RAS) −− the world's first web−based system for tracking the activities of drug counterfeiters. The Rapid Alert System communications network will transmit reports on the distribution of counterfeit medicine to the relevant authorities for them to take rapid countermeasures. National health authorities and other partner agencies will be linked to the system. "We hope that the Rapid Alert System will considerably strengthen our hand against the counterfeiters," said Budiono Santoso, WHO's Regional Adviser in Pharmaceuticals for the Western Pacific Region. "Rapid communication and efficient exchange of information are crucial to combating counterfeiting." Between six percent and 10 percent of medicine on the world market is reported to be counterfeit with estimated sales of over $35 billion a year. Counterfeit medicine is often distributed across national boundaries. Effective measures to protect people from counterfeit drugs require collaboration and coordination among relevant stakeholders in each country, between member countries, and relevant partner organizations.
Source: http://www.wpro.who.int/media_centre/press_releases/pr_20050 503.htm

20. *May 03, United Press International* — **Ambulances, paramedics shut out of funding.** Emergency medical−services (EMS) departments, which run the nation's ambulances and paramedics, are losing out on federal funding and other support because they are overseen by the Department of Transportation (DOT), not the Department of Homeland Security (DHS), according to a report released Tuesday, May 3. Federal oversight of and support for emergency medical services is "buried deep in the bureaucracy" of the DOT's National Highway Traffic Safety Administration, the George Washington University report finds, making it "an all−but−forgotten component of emergency response." The report, written by a task force of emergency medical−services leaders set up by the university's Homeland Security Policy Institute, says that because of this "lack of federal leadership" EMS departments are not getting the federal funding they need. "Although EMS providers are roughly equal in numbers to firefighters and law enforcement officers, they receive only four percent of the first responder funding allocated by DHS," states the report. The report recommends the establishment of an Emergency Medical Services Administration, analogous to the Fire Administration, which oversees and funds fire departments nationwide.
Emergency Medical Services report:
http://hspi.gwu.edu/reports/HSPI_EMS_Report_5−2−05.pdf

Source: http://www.upi.com/view.cfm?StoryID=20050503−080457−3377r

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

21. *May 04, Daily Record* — **Drill conducted at Three Mile Island.** Emergency responders from areas that surround Three Mile Island (TMI) nuclear power plant in Dauphin County, PA, took part in a dry run Tuesday, May 3, that evaluated how officials would respond to a plant−borne radiologic crisis. AmerGen Energy, the utility that operates TMI, created the scenario, which involved a plant malfunction leading to a release of radioactive material into the atmosphere. Every other year, Federal Emergency Management Agency (FEMA) officials evaluate how local emergency operation centers located within 10 miles of TMI would function in the event of a real radiologic crisis. Following the exercise, FEMA will send its final evaluation report to the Nuclear Regulatory Commission (NRC) within 90 days of the exercise and the report will be available to the public within 120 days. The NRC uses the data in its licensing decisions regarding nuclear power plants, said Niki Edwards, a FEMA spokesperson. State and federal officials will discuss the preliminary findings of Tuesday's Radiological Emergency Preparedness Exercise for Three Mile Island at a public meeting slated for noon Friday at Four Points Sheraton in Harrisburg.
Source: http://ydr.com/story/business/67753/

22. *May 03, Star Courier (IL)* — **Disaster exercise involves area emergency services.** Law enforcement, ambulance personnel and local and area fire departments in Kewanee, IL, took part in the four−hour drill, which started with a report of a suspicious person near the Hotel Kewanee on Saturday April 30. Kewanee police tailed the person to the hotel basement, where they reported a noticeable odor coming from inside the building. The Henry County SWAT team was called in after the "suspicious subject" told police he had taken several hostages. After a hostage negotiator exhausted all available options, multiple gunshots were heard from the basement. The tactical teams entered the building and found mass casualties, hazardous materials from an active meth lab and a missing shooter. After police said the crime scene had been secured, the SWAT team emerged with a man in handcuffs and reported the presence of hazardous materials. Firefighters got on the mutual aid broadcast system and requested a hazardous materials (hazmat) team. The team set up the procedure for entry, science and decontamination. The final stage of the drill was at Kewanee Hospital, where patients were run through the hospital's decontamination tent at the emergency room entrance.
Source: http://www.starcourier.com/articles/2005/05/03/city/city1.tx t

23. *May 03, Daily Local (PA)* — **Classes teach awareness training on weapons of mass destruction.** Since November, officials from the Department of Emergency Services in Chester County, PA, have been organizing classes in awareness training on weapons of mass

destruction for police and ambulance workers. The class is an introduction to all weapons of mass destruction, including chemical, radiological and biological agents. Participants learn how to properly put on suits to protect them from exposure to harmful materials, and also about the weapons' effects and their methods of dispersion. Tony Przychodzien Jr., the department's grant and planning coordinator, said the goal is to provide training to every police officer and emergency services worker in the county. "A lot of chemical agents are reviewed," said Przychodzie. "It's a knowing introduction to weapons of mass destruction." Upon completion of the course, every participant receives a Millenium kit, which contains a mask, boots, gloves and a full−body suit. Instructors teach how to properly seal the suit so there is no exposure to dangerous elements. Przychodzien said 561 police and EMS workers have been trained since November. About 98 percent of the police in the county have received training.
Source: http://www.dailylocal.com/site/news.cfm?newsid=14457913&BRD=1671&PAG=461&dept_id=17782&rfi=6

[Return to top]

Information Technology and Telecommunications Sector

24. *May 04, Associated Press* — **American Tower to acquire SpectraSite.** Communications tower management firm American Tower Corp. said Wednesday, May 4, it agreed to pay $3.1 billion in stock to acquire rival SpectraSite Inc., a Cary, NC−based operator of wireless and broadcast signal towers. The transaction is expected to close in the second half of 2005, subject to shareholder and regulatory approvals. Following the closing, the combined company will have a portfolio of more than 22,600 communications sites in the U.S., Brazil and Mexico and annual revenue of more than $1 billion.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/05/04/AR2005050400508.html

25. *May 03, FrSIRT* — **Apple security update fixes multiple Mac OS X vulnerabilities.** Apple has released a security patch to correct twenty vulnerabilities affecting Mac OS X. The flaws can be exploited by remote or local attackers to execute arbitrary commands, cause a denial of service or obtain elevated privileges. Apply Security Update 2005−005 (Client): http://www.apple.com/support/downloads/securityupdate2005005 client.html or Security Update 2005−005 (Server): http://www.apple.com/support/downloads/securityupdate2005005 server.html
Source: http://www.frsirt.com/english/advisories/2005/0455

26. *May 03, FrSIRT* — **HP OpenView Event Correlation Services unspecified vulnerabilities.** A remote user can execute arbitrary code with elevated privileges and can cause denial of service conditions.
Apply patches: http://www.itrc.hp.com
Source: http://www.frsirt.com/english/advisories/2005/0451

27. *May 03, FrSIRT* — **HP OpenView Network Node Manager unspecified vulnerabilities.** Two vulnerabilities were identified in HP OpenView Network Node Manager, which could be exploited by remote attackers to execute arbitrary commands or cause a denial of service. A

remote user can execute arbitrary code with elevated privileges and can cause denial of service conditions. Apply patches: http://www.itrc.hp.com
Source: http://www.frsirt.com/english/advisories/2005/0450

28. *May 03, Secunia* — **osTicket multiple vulnerabilities.** The vulnerabilities in osTicket, which can be exploited by malicious users to conduct SQL injection attacks, and by malicious people to conduct cross−site scripting and script insertion attacks, disclose sensitive information and compromise a vulnerable system. Input isn't properly sanitized before being returned to the user. The vulnerabilities have reportedly been fixed by the vendor.
Source: http://secunia.com/advisories/15216/

29. *May 03, Secunia* — **SitePanel multiple vulnerabilities.** The vulnerabilities in SitePanel, which can be exploited by malicious people to conduct cross−site scripting attacks, disclose sensitive information and compromise a vulnerable system. Input isn't properly sanitized before being returned to the user. Update to version 2.6.1.1:
http://sitepanel2.com/phpaudit/client_area_login.php
Source: http://secunia.com/advisories/15213/

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: Apple has released a security patch to correct twenty vulnerabilities affecting Mac OS X. These flaws could be exploited by remote or local attackers to execute arbitrary commands, cause a denial of service or obtain elevated privileges.

Current Port Attacks

Top 10 Target Ports	[fetch Target Ports (auto)] [fetch Target Ports (manual)]

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

30. *May 04, Associated Press* — **Senior al Qaeda suspect arrested, Pakistan says.** Pakistan authorities arrested the nation's most−wanted militant, the head of al Qaeda operations in Pakistan who had a $10 million bounty on his head, and said Wednesday, May 4, they now were "on the right track" to catch Osama bin Laden. Abu Farraj al−Libbi, who allegedly orchestrated two assassination attempts against President Pervez Musharraf, was arrested after a firefight on the outskirts of Mardan, 30 miles north of Peshawar, capital of the deeply conservative North West Frontier Province, the government and security officials said. Al−Libbi, a native of Libya who authorities say is a close associate of bin Laden, was arrested earlier this week, Information Minister Sheikh Rashid Ahmed said.
Source: http://www.usatoday.com/news/world/2005−05−04−pakistan−arrest_x.htm?POE=NEWISVA

[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:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.