Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 22 April 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Computing reports online retailers will be forced to tighten security and improve their handling of customer data under new rules being introduced in June by the credit card industry to stop identity theft (See item 4)
- MSNBC reports Ameritrade Inc. has advised 200,000 current and former customers that a computer backup tape containing their personal information has been lost. (See item 6)
- The Washington Post reports the U.S. government plans to insist that foreign airlines flying over American soil turn over the names of passengers on board or check the names against U.S. government watch lists in an effort to prevent terrorists from entering U.S. airspace. (See item 9)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; 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 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. *April 21, Independent System Operator New England* — **Power agency projects adequate power supplies in New England.** Independent System Operator (ISO) New England Inc., the operator of New England's bulk power system and wholesale electricity markets, on Thursday, April 21, issued its summer 2005 electricity supply outlook. Although regional electricity use could reach record−breaking levels this summer, ISO New England is forecasting that adequate

supplies will be available to meet demand. However, local transmission constraints, extremely hot days or unexpected transmission or generation outages could require the implementation of emergency measures to help maintain power system reliability. Regional electricity use may reach an all−time high this summer and could surpass the established New England record for electricity use by up to 10 percent. Although the region as a whole is expected to have adequate supply to meet demand, bulk power system inadequacies in Southwest Connecticut could create reliability problems for that area. Extreme weather, unforeseen outages or localized transmission constraints in Greater Boston could also create electricity reliability concerns for that area this summer.
Source: http://www.iso−ne.com/iso_news/2005_Archive/2005_Summer_Capa city_Release.pdf

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *April 21, Los Angeles Times (CA)* — **Two hospitalized after ammonia leak.** An ammonia leak discovered by workers repairing a 3,000−gallon ammonia tank at the Diamond Newport Ice Company in Santa Ana, CA, Wednesday, April 20, prompted the evacuation of dozens of employees, two of whom were hospitalized, fire officials said. One worker suffered burns on his arm and a second complained of shortness of breath after inhaling fumes, said Santa Ana Fire Capt. Dave Thomas. Neither of the workers was identified.
Source: http://www.latimes.com/news/local/orange/la−me−ocbriefs21apr21,1,1118973.story?coll=la−editions−orange

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *April 21, Associated Press* — **Carnegie Mellon says computers breached.** Carnegie Mellon University, located in Pittsburgh, PA, is warning more than 5,000 students, employees and graduates that their Social Security numbers and other personal information may have been accessed during a breach of the school's computer network. Carnegie Mellon discovered the breach on April 10. Spokesperson Mike Laffin said that as of Wednesday, April 20, the school had no clear idea how long the system had been vulnerable. Officials say they have no evidence that anyone had used the personal information.
Source: http://www.washingtonpost.com/wp−dyn/articles/A6646−2005Apr2 1.html

4. *April 20, Computing* — **E−commerce sites forced to adopt security standards.** Online retailers will be forced to tighten security and improve their handling of customer data under new rules being introduced by the credit card industry to stop identity theft. Beginning June 30, all e−commerce sites with internal systems that process, store or transmit cardholder

information will have to comply with the Payment Card Industry (PCI) Data Security Standard or face significant fines. Backed by MasterCard, Visa, American Express, Diners Club and JCB Cards, the standard requires Internet retailers to carry out a 12−step security audit, which will be certified annually and checked every three months. The PCI Data Security Standard will also help converge the different security standards demanded by Visa, MasterCard and American Express, says Avivah Litan, research director at Gartner, a provider of research and analysis on the global IT industry. The credit card industry hopes the tighter security demanded by the standard will lead to fewer stolen credit card numbers circulating on the Internet.
Payment Card Industry Data Security Standard:
http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf
Source: http://www.computing.co.uk/news/1162594

5. *April 20, IT Week* — **Police fail to cope with e−crime.** Firms need to step up their IT security to prevent attacks, as police are unable to cope with the growing problem of computer crime. This was the message given to delegates at April's E−Crime Congress in London. Howard Schmidt, eBay's chief security strategist and a former security advisor to the White House, warned delegates that law enforcement agencies do not have enough resources to cope with the increasing amount of electronic crime. As a result, organizations should do more to protect themselves, according to Schmidt. The UK National Hi−Tech Crime Unit (NHTCU), which hosted the event, said that more cooperation between law enforcement agencies and industry is needed. Len Hynds, outgoing head of the NHTCU, called on big businesses to "put aside personal and aspirational agendas" and share their expertise and knowledge of IT crime prevention with police.
E−Crime Congress 2005: http://www.e−crimecongress.org/ecrime2005/website.asp
Source: http://www.itweek.co.uk/news/1162578

6. *April 19, MSNBC* — **Ameritrade warns clients of lost data.** Ameritrade Inc. has advised 200,000 current and former customers that a computer backup tape containing their personal information has been lost. The tape contained information spanning the years 2000−2003, and included both current and past consumers of the online broker, according to spokesperson Donna Kush. Notices were mailed to the affected consumers last week, according to the company. "We believe that information about your closed account resided on the missing tape," read one typical message, sent to a former Ameritrade customer. "The information could include your account number, name and/or other personal information, like your Social Security number." The letter also says that the missing tape was "likely lost or was destroyed." The online broker has over 3.7 million current customers, Kush said. A total of four backup tapes were found to be missing from a box that was damaged during shipping between two facilities, the company said. Three of the four tapes have been recovered at the shipper's facility. "We don't believe any foul play was involved," Kush said.
Source: http://www.msnbc.msn.com/id/7561268/

[Return to top]

Transportation Sector

7.

April 21, Associated Press — **Organizers: Minuteman Project successful.** The organizers of a group of volunteers patrolling the Mexican border for illegal immigrants are declaring the Minuteman Project a success before it is even over. But others say it has done little more than make noise. There have been no reports of any vigilante violence, as law enforcement authorities feared when the volunteers took up positions at the start of April. About 750 volunteers have spent at least one eight−hour shift in the field, patrolling a 23−mile stretch of desert between Naco and Douglas, AZ, to try to stem the flow across the busiest illegal entry point on the Mexican border. "In just 17 days, the Minuteman Project has successfully sealed the San Pedro River Valley border from illegal activity," Minuteman organizer Jim Gilchrist said on the project's Website. But Michael Nicley, chief of the U.S. Border Patrol's Tucson sector, which encompasses most of the Arizona border, and others attributed the drop to U.S. agents and the increased presence of Mexican police and members of Grupo Beta, a Mexican government−sponsored organization that tries to discourage people from crossing illegally and aids those stranded in the desert.
Minuteman Project Website: http://www.minutemanproject.com/
Source: http://story.news.yahoo.com/news?tmpl=story&cid=519&ncid=718&e=2&u=/ap/20050421/ap_on_re_us/border_volunteers

8. *April 21, Associated Press* — **Amtrak's Acela sidelined until summer.** Amtrak will not be able to run any of its high−speed trains until the summer because of delays in getting replacement parts to correct brake problems on Acela Express cars, railroad officials said Wednesday, April 20. "The earliest you'll see trains back in service will be sometime in the summer and then you'll see a gradual return," said Amtrak's chief executive officer, David Gunn. Before Amtrak's showcase service resumes, Amtrak's chief operating officer, Bill Crosbie, said there must be agreement on how long the new brakes will last. The brakes were to last one million miles; the current Acela fleet had about half of that mileage. Amtrak pulled all of its 20 Acela trains out of service on Friday, April 15, after finding millimeter−size cracks in 300 of the fleet's 1,440 disc brake rotors. Each Acela train has 72 brakes. "This part is unique to the Acela and there is no active production line casting them," said Crosbie said. "The manufacturer has told me this will take some time." The brake problem surfaced when a Federal Railroad Administration worker performed a routine inspection April 14 after a high−speed run to test whether Amtrak could speed up the Acela trains slightly on curves between Trenton and Newark, NJ.
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−amtrak−acela,0,1856189.story?coll=sns−ap−nation−headlines

9. *April 21, Washington Post* — **Passenger lists sought for flights over U.S.** The U.S. government plans to force foreign airlines flying over American soil to turn over the names of passengers on board or check the names against U.S. government watch lists in an effort to prevent terrorists from entering U.S. airspace. Under current rules, overseas carriers are required to provide passenger manifests to U.S. officials within 15 minutes of takeoff if they are to land in the United States, according to the Transportation Security Administration (TSA). Officials have been concerned that terrorists may try to hijack a plane over the United States and crash it into a building, as occurred on September 11, 2001. "We are currently considering a measure that would require foreign carriers to vet their passenger manifests against the 'no−fly' list and 'selectee' lists on overflights," said TSA spokesperson Yolanda Clark. The no−fly list is a secret list of thousands of names of known or suspected terrorists who may pose

a threat to U.S. aviation. The selectee list contains the names of individuals who are not known terrorists but present a possible threat to the airplane. The proposal has angered European, Mexican and Canadian airlines, which operate most of the 500 estimated daily overflights. If foreign airlines do not comply with the order, which is expected to be issued in coming weeks, they could have to reroute flights, adding time and cost to the journeys.
Source: http://www.washingtonpost.com/wp−dyn/articles/A6015−2005Apr2 0.html

10. *April 21, Huntsville Times (AL)* — **Mock airline disaster drill.** A mock airline disaster drill was held starting at 9 a.m., Thursday, April 21, at the Huntsville, AL, International Airport to test the area's public safety personnel. Every three years, the Federal Aviation Administration requires major airports to conduct disaster drills to test emergency responses for communication, fire and police, emergency medical, hospital multiple casualties plans, mutual aid and the incident command system, said Cindy Maloney, airport spokesperson. This year's drill also was a training experience for local Community Emergency Response Teams (CERT), said Scott Worsham, Huntsville−Madison County Emergency Management Agency officer and CERT program coordinator.
Source: http://www.al.com/news/huntsvilletimes/index.ssf?/base/news/1114075147174690.xml

[Return to top]

Postal and Shipping Sector

11. *April 21, News and Sentinel (WV)* — **Fraudulent money orders found in West Virginia.** An Internet fraud scheme that passes counterfeit postal money orders as real has made its way to the Mid−Ohio Valley, officials said. "The Mineral Wells, WV, Post Office had an incident of the counterfeit money orders a few weeks ago," said Bill Amick, postmaster. "The money orders have been found all over the state and people are losing a lot of money because of them," said Tony Branch, postal inspector in Clarksburg. According to U.S. postal inspectors, the counterfeit money order scam begins when a victim is contacted by someone through an Internet chat room or online auction site claiming to have financial problems or needing help to cash domestic and/or international postal money orders. The person in need often claims to be living in a foreign country (usually Nigeria), but the scam can come from any location. The scam artist is looking to recruit someone in the U.S. to cash the money orders and return the funds via wire transfer. U.S. residents are lured into the scam when they are told they can keep some of the money as a gift or payment for their help.
Source: http://www.newsandsentinel.com/news/story/0421202005_new03_m oneyorders.asp

[Return to top]

Agriculture Sector

12. *April 21, BBC News* — **Rice fungus genome mapped.** Scientists have unraveled the genome of the rice plant's most severe fungal threat. Magnaporthe grisea (M. grisea) is the first pathogenic plant fungus to have its life−code mapped, which could pave the way for new treatments of the disease. "Controlling rice blast disease (M. grisea) is for the first time a

realistic prospect," said Nick Talbot, from Exeter University, who was part of the team sequencing the genome. M. grisea comprises of windborne spores that stick to the leaves of the rice plant. As it germinates, the spore forms a dome−shaped structure called an "appressorium," or pressure cell, whose task it is to infect the plant. The tiny organ produces extraordinary pressures to drive a penetrative peg beneath the leaf's protective waxy surface. In young seedlings, rice blast often destroys the whole plant; in older plants, the grain is lost. It is estimated that, every year, the rice blast fungus kills an amount of rice that would feed 60 million people. M. grisea's cousins also attack some 50 other kinds of grass plants, including wheat, barley, and millet. Details of the rice blast sequence have revealed that the fungus produces a group of proteins which may be highly susceptible to new fungicides.
Source: http://news.bbc.co.uk/1/hi/sci/tech/4466783.stm

[Return to top]

Food Sector

13. *April 20, Associated Press* — **Thousands of Waffle House diners possibly exposed to hepatitis.** Health officials are offering free shots to people who ate at an eastern Tennessee restaurant where a food server was infected with hepatitis A. The restaurant estimates as many as 5,000 people who ate at the Waffle House in Clinton between April 5 and 15 may have been exposed to the viral liver disease. Officials still aren't sure of the source of the outbreak. They've confirmed 17 cases of hepatitis A in recent weeks, including in the Waffle House worker.
Source: http://www.thenewmexicochannel.com/health/4396653/detail.htm l?tabbox=health

14. *April 20, Food Safety and Inspection Service* — **Salmonella cases linked to frozen chicken entrees.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) is issuing a public health alert to remind consumers to ensure that frozen meat and poultry products are fully cooked before they are consumed. FSIS has linked cases of Salmonella infections in people to stuffed frozen chicken products sold in Minnesota and Michigan. FSIS is working with the Centers for Disease Control and Prevention (CDC) and officials in Michigan and Minnesota to identify the source of the infections and to ascertain whether the chicken products are the sole source of the illnesses. Food contaminated with Salmonella can cause salmonellosis, one of the most common bacterial foodborne illnesses.
Source: http://www.fsis.usda.gov/News_&_Events/NR_042005_01/index.as p

[Return to top]

Water Sector

15. *April 20, Associated Press* — **West's water troubles getting worse, officials say.** As the western U.S. enters its sixth year of a record dry spell, federal and state officials are scrambling to come up with a viable solution to the region's water dilemmas. Western policy makers, scholars, environmentalists and industry representatives gathered in Boise, ID, on Tuesday, April 19, for a two−day forum to discuss the water issues that are plaguing the region. Officials revealed during the discussion that the drought issue has served as a wake−up call to examine

water use in the West and the potential need for new dams. Officials are urging increased water conservation, but regulated conservation could have an impact on the region as well. Over−irrigation by farmers in Idaho's Lemhi Valley recharges the alluvial aquifer that keeps the Lemhi River flowing during months it normally would be dry, and if conservation were ordered, "we wouldn't have the salmon we've got there now," according to Karl Dreher, director of the Idaho Department of Water Resources.
Source: http://www.azcentral.com/news/articles/0420waterwoes−ON.html

[Return to top]

Public Health Sector

16. *April 21, Daily Mail (United Kingdom)* — **Dutch report first human case of mad cow disease.** A 26−year−old Dutch woman has been diagnosed with variant Creutzfeldt−Jakob Disease (vCJD), health authorities have said, the first known human case of the fatal disease in the Netherlands. Seventy−seven Dutch cows are known to have been infected since 1997 with bovine spongiform encephalopathy, known as mad cow disease, which is believed to cause vCJD in humans. The patient, whose name was not released, is believed to have contracted the disease by eating tainted beef, the Health Ministry said in a statement. Bas Kuik, a spokesperson for the Health Ministry, said the woman, who has never lived outside the Netherlands, was likely to have been infected before 1997, when the country introduced tight restrictions on beef imports after a wave of mad cow cases in Britain.
Source: http://www.dailymail.co.uk/pages/live/articles/health/thehealthnews.html?in_article_id=345829&in_page_id=1797

17. *April 21, Los Angeles Times (CA)* — **Angola sends medical teams to fight Marburg virus.** Authorities are sending a team of 30 doctors and nurses to a northern Angolan city to help fight the deadly Marburg virus which has claimed 237 lives, Health Minister Sebastiao Veloso said Thursday, April 21. The team −− made up of all volunteers from the capital, Luanda −− was to join other medical staff in Uige, including those from international organizations, Veloso said. Almost all the deaths from the rare Ebola−like virus have occurred in Uige, a city 180 miles north of Luanda. Several victims who died in other areas of the country had previously been in Uige.
Source: http://www.latimes.com/news/nationworld/nation/wire/ats−ap_health13apr21,1,4981122.story?coll=sns−ap−tophealth&ctrack=1& cset=true

18. *April 20, Associated Press* — **All samples of deadly flu virus found.** All samples of the deadly influenza virus sent outside the U.S. have been destroyed except for one in Lebanon, the World Health Organization (WHO) agency said Wednesday, April 20. The sample that had gone missing in Beirut, Lebanon, "was found at the airport," said Maria Cheng, spokesperson for the WHO. Previously unaccounted for samples sent to Mexico and South Korea already have been destroyed, she said. Walid Ammar, director general of Lebanon's Health Ministry, said that the sample was being kept "in a safe place" until the ministry was instructed on whether to destroy it or send it back to the College of American Pathologists. Cheng said WHO had contacted the College of American Pathologists "to see if they would accept this package back or if they wanted to ship it to another lab to be destroyed." Cheng said South Korean officials had previously reported to WHO that they had destroyed half the samples they had

been sent, but hadn't confirmed they also destroyed the other half. The destruction of all the samples sent to South Korea has now been confirmed, she said. A missing shipment to Mexico has been tracked down in a warehouse and has also been destroyed, she added.
Source: http://www.nytimes.com/aponline/international/AP−Pandemic−Flu−Labs.html?oref=login

[Return to top]

Government Sector

19. *April 21, Associated Press* — **Court officials call for homeland security funding.** A national group of court officials called Thursday, April 21, for Congress to earmark a share of federal homeland security dollars for increased protection at state and local courthouses. The officials, including judges and bailiffs, said states do not currently set aside money for courthouse security on their own. The earmark request was a prevailing theme Thursday at a summit on court security hosted by the National Center for State Courts. Although the event had been planned for months, it was moved up in response to last month's courtroom shooting in Atlanta in which a suspect shot and killed a judge and three others. Brian Nichols, who was arrested after an intense manhunt, was shackled at the ankles when he appeared before a judge in Atlanta's Fulton County Courthouse last week −− a precaution that hadn't been taken the day of the crime. "Court security is just not on somebody's radar screen until you have these tragedies," said Mary McQueen, president of the National Center for State Courts. McQueen said little if any of the federal homeland security money that goes to states in the form of block grants is being used for courtrooms.
Source: http://www.cnn.com/2005/LAW/04/21/courthouse.security.ap/

20. *April 21, Asbury Park Press (NJ)* — **Second bomb threat at courthouse.** Monmouth County, NJ, Courthouse operations were disrupted for a second day when a caller reported a bomb in the courthouse early Wednesday morning, April 20. Between 8:35 and 8:40 a.m., a 911 call was made to the Monmouth County Sheriff's Office communication division from a caller reporting a bomb, Monmouth County Undersheriff Theodore Freeman said. The 490 court employees were evacuated and told the courthouse would reopen at 4 p.m. Freeman said the courthouse was closed for the remainder of the day. Bomb−sniffing dogs from the Monmouth County Sheriff's Office and numerous other agencies including the State Police, Department of Corrections, Port Authority of New York and New Jersey and five other county Sheriff's offices searched the building and found no device, Freeman said. At 9:35 a.m. Tuesday, the trial court administrator's office received a threat from a male caller announcing a bomb threat at the courthouse and or Hall of Records. Both buildings were evacuated, searched and reopened later that day.
Source: http://www.app.com/apps/pbcs.dll/article?AID=/20050421/NEWS01/504210374/1004/NEWS01

[Return to top]

Emergency Services Sector

21. *April 21, Florida Today* — **Rescue personnel train for terror attacks.** On Wednesday, April 20, dozens of first responders performed rescue drills wearing cumbersome gear at Brevard Community College's campus in Cocoa, FL. Participants wore green rubber gloves and boots, white hooded Tyvek bodysuits and black air masks, their seams sealed airtight with tape. Instructors from the University of Miami conducted the terrorism course, ordering the 43 students to spend hours in their outfits, carry dummies on litters and perform simulated medical procedures. During another drill, participants had to administer IV needles and insert breathing tubes into rubber arms and mouths. Some workers fumbled with their gloves during these tasks. Classes continued Thursday with triage exercises and instruction on chemical, radiological and biological agents. During the past 18 months, the University of Miami program has trained about 1,100 emergency personnel in Miami and almost 700 more in traveling scenarios from Pensacola to Marathon. The effort receives funding from the Florida Department of Health. Thursday's exercise was the latest in a sequence of Brevard terrorist attack preparations in the aftermath of the 9−11 attacks.
Source: http://www.floridatoday.com/apps/pbcs.dll/article?AID=/20050421/NEWS01/504210337/1006

22. *April 21, Pioneer Press (MN)* — **Alert system fell silent during school shooting.** Although Red Lake Senior High School in Red Lake, MN, had an emergency response plan in place, teachers and students weren't warned after Jeff Weise shot his way into the building last month, school officials said. While the emergency plan calls for warnings to be broadcast over the school's intercom, that warning never came, and officials aren't sure why, said Carol Aenne, the school district's acting superintendent. Interviews with school officials and others indicated that initiative on the part of individual teachers −− not the formal response plan −− helped protect faculty and students. Teachers heard gunshots and locked themselves and their students in their classrooms, despite the sounding of the school's fire alarm, which was a signal for them to evacuate, said Aenne. Red Lake tribal police officers went to the school after the department got 911 calls from those in the building. Pat Mills, director of public safety on the Red Lake reservation, said so many 911 calls came in that they overloaded the department's phone system and shut it down. "We're going to ratchet up our drills so that it becomes second nature as far as responsibilities of the crisis−management team in each building," Aenne said. "We're also going to have reports, weekly reports, from the building principals as to their progress on tabletop drills and actual drills."
Source: http://www.twincities.com/mld/twincities/news/local/11446709 .htm

23. *April 20, Local10.com* — **Boaters asked to watch for orange cards.** Scientists are hoping that boaters and beachcombers who find orange cards floating in the water will get in touch with researchers. The orange cards represent an oil spill. They were part of an emergency response drill conducted by the National Oceanic and Atmospheric Administration (NOAA) off the coast of Key Largo Wednesday, April 20. The drill simulated the grounding of an 800−foot cargo vessel, and the cards simulate how oil might drift away from such a grounding. Each card has written instructions in English and Spanish that explain how to report where it was found.
Report a drift card to NOAA: http://response.restoration.noaa.gov/driftFL.html
Source: http://www.local10.com/news/4399571/detail.html

[Return to top]

Information Technology and Telecommunications Sector

24. *April 21, New York Times* — **Time Warner and Comcast acquire Adelphia Communications.** Time Warner and its bidding partner, Comcast, said Thursday, April 21, that they had reached an agreement to acquire Adelphia Communications for a total of $12.7 billion. Adelphia, the fifth−largest cable TV operator in the United States, has been in bankruptcy protection since 2002, and the deal is subject to the customary regulatory review and the bankruptcy judge. Time Warner and Comcast said they expected the deal to close in nine to 12 months. Comcast will get 1.8 million cable subscribers, bringing its total to about 23.3 million. Time Warner Cable will get about 3.5 million basic subscribers bringing its total to about 14.4 million. The deal will give Time Warner and Comcast control of Adelphia's 5.3 million subscribers in 31 states, including systems around Los Angeles and in upstate New York.
Source: http://www.nytimes.com/2005/04/21/business/21cnd−adelphia.html?hp&ex=1114142400&en=217775ddf1576100&ei=5094&partner=home page

25. *April 20, FrSIRT* — **phpBB−Auction SQL injection and path disclosure vulnerabilities.** Two vulnerabilities were reported in phpBB−Auction, which may be exploited by attackers to execute arbitrary SQL commands or disclose the full web path. 1. The flaw is due to an SQL injection error in the "auction_rating.php" and "auction_offer.php" scripts when handling specially crafted "u" and "ar" parameters. 2. The vulnerability is due to an input validation error in the "auction_myauctions.php" script when handling a specially crafted "mode" parameter, which may be exploited to display the installation path. There is no solution at this time.
Source: http://www.frsirt.com/english/advisories/2005/0372

26. *April 20, FrSIRT* — **Sun Java System Web Proxy Server buffer overflow vulnerabilities.** A new vulnerability was identified in Sun Java System Web Proxy Server, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an unspecified buffer overflow error which may allow a remote attacker to compromise a vulnerable system and execute arbitrary code with the privileges of the server process. Note: The default UID for the Web Proxy Server is "nobody".
Upgrade to Sun Java System Web Proxy Server 3.6 Service Pack 7 or later: http://www.sun.com/download/index.jsp
Source: http://www.frsirt.com/english/advisories/2005/0367

27. *April 20, FrSIRT* — **Apple iSync "mRouter" local buffer overflow vulnerability.** A new vulnerability was identified in Apple Mac OS X, which could be exploited by local attackers to obtain elevated privileges. This flaw is due to a buffer overflow error in the iSync helper tool mRouter when handling specially crafted command line arguments, which can be exploited by a malicious user to execute arbitrary commands with "root" privileges.
Security Update 2005−004: http://wsidecar.apple.com/cgi−bin/nph−reg3rdpty1.pl/product=05661&platform=osx&method=sa/SecUpd2005−004Pan.dmg
Source: http://www.frsirt.com/english/advisories/2005/0366

28. *April 20, IDG News Service* — **Cyber attack early warning center begins pilot project.** A fledgling nonprofit group working to develop an automated cyber−attack early warning system, the Cyber Incident Detection Data Analysis Center (CIDDAC), is about to begin a pilot project

to collect data on network intrusions from a group of companies in national−infrastructure industries. Backed by a grant from the Department of Homeland Security, CIDDAC has set up an operations center at the University of Pennsylvania's Institute of Strategic Threat Analysis and Response laboratory. Around 30 organizations will eventually participate in the project, although some are still being selected, according to CIDDAC Executive Director Charles Fleming. He expects to have useful data from the pilot test in about five months. CIDDAC's focus is on linking together organizations in industries such as banking, electrical power, gas and oil, telecommunications and transportation. The center will use a network of sensors, dubbed RCADSs (Real−Time Cyber Attack Detection Sensors), to gather information on intrusions and attempts. CIDDAC will also pass collected information on to law enforcement agencies, but Fleming emphasized that serving private−sector alert needs is the group's priority.
CIDDAC Website: http://www.ciddac.org/
Source: http://www.infoworld.com/article/05/04/20/HNcyberpilot_1.htm l

29. *April 20, CNET News* — **Trojan horses take aim at Symbian cell phones.** The recent discovery of a large number of malicious mobile phone programs should raise concerns throughout the wireless industry, according to a virus tracker. Cell phone antivirus software company SimWorks reported Wednesday, April 20, that 52 new Trojan horses are hidden inside several different cell phones games and other readily available mobile phone software. While the software appears to be safe to share or use, the Trojans actually contain malicious software that crashes many critical cell phone system components. The Trojan horses target only cell phones that use Symbian, an advanced operating system. To date, no phones have been affected, according to Aaron Davidson, chief executive officer of SimWorks. While the damage is negligible so far, the recent warnings from SimWorks and security specialist F−Secure are raising alarm bells in the wireless industry. The latest report brings the total number of known Symbian Trojan horses to more than 100.
Source: http://news.com.com/Trojan+horses+take+aim+at+Symbian+cell+p hones/2100−7349_3−5678211.html

30. *April 15, Government Accountability Office* — **GAO−05−276: Information Technology: OMB Can Make More Effective Use of Its Investment Reviews (Letter Report).** For the President’s Budget for Fiscal Year 2005, the Office of Management and Budget (OMB) stated that of the nearly 1,200 major information technology (IT) projects in the budget, it had placed approximately half—621 projects, representing about $22 billion—on a Management Watch List, composed of mission−critical projects with identified weaknesses. The Government Accountability Office (GAO) was asked to describe and assess OMB’s processes for (1) placing projects on its Management Watch List and (2) following up on corrective actions established for projects on the list. To enable OMB to take advantage of potential benefits of using its Management Watch List as a tool for analyzing, setting priorities, and following up on IT projects, GAO made recommendations to OMB aimed at more effective development and use of its Management Watch List. In commenting on a draft of this report, OMB did not agree that an aggregated list, as recommended by GAO, is necessary for adequate oversight and management, because it uses other information and processes for this purpose. However, GAO continues to believe that an aggregated list would contribute to OMB’s ability to analyze IT investments governmentwide and track progress in addressing deficiencies.
Highlights: http://www.gao.gov/highlights/d05276high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−276

31. *April 06, Government Accountability Office* — **GAO−05−257: Telecommunications: Direct Broadcast Satellite Subscribership Has Grown Rapidly, but Varies across Different Types of Markets (Letter Report).** Since its introduction in 1994, direct broadcast satellite (DBS) service has grown dramatically, and this service is now the principal competitor to cable television service. Although DBS service has traditionally been a rural service, passage of the Satellite Home Viewer Improvement Act of 1999 enhanced the competitiveness of DBS service in suburban and urban markets. The Government Accountability Office (GAO) agreed to examine DBS subscribership and DBS penetration rates since 2001. GAO found that since 2001, the number of households subscribing to DBS service has grown rapidly; thus the percentage of households subscribing to DBS service, the DBS penetration rate, has grown to over 17 percent of American households. The DBS penetration rate is highest in rural areas, but growing most rapidly in suburban and urban areas. The degree and type of competition influences the DBS penetration rate. In addition to the differences in DBS penetration rates across rural, suburban, and urban areas, and differences associated with the degree and type of cable competition, additional geographic and competitive factors also influence the DBS penetration rate.
Highlights: http://www.gao.gov/highlights/d05257high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−257

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: Multiple vulnerabilities have been reported in Firefox, which can be exploited by malicious people to conduct cross−site scripting attacks, bypass certain security restrictions, and compromise a user's system. Successful exploitation may allow execution of arbitrary code.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 41170 (−−−), 4662 (eDonkey2000), 6346 (gnutella−svc), 1026 (−−−), 139 (netbios−ssn), 53 (domain), 1027 (icq), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

32. *April 19, Department of State* — **Travel warning issued for Tunisia.** A public announcement is issued by the Department of State to alert Americans to the potential for terrorist actions in Tunisia. The public announcement expires on July 19, 2005. The United States Government has strong indications that individuals may be planning imminent terrorist actions in Tunisia. No further information on specific targets, timing, or method of attack, or capabilities of these individuals is available. In the past, terrorists have not distinguished between official and civilian targets. Terrorist attacks may occur on or around dates of religious significance, such as the Moulid holiday in the third week of April. U.S. Government facilities remain at a heightened state of alert. Americans in Tunisia are urged to remain vigilant with regard to their personal security and to exercise caution.
Source: http://travel.state.gov/travel/cis_pa_tw/pa/pa_2258.html

[Return to top]

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.

DHS/IAIP Disclaimer