Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 02 May 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The alleged ring leader of a plot to steal 500,000 bank accounts and personal information and sell the data to bill collectors appeared in New Jersey court last last week; Orazio Lembo's alleged accomplices included branch managers and employees from some of the state's biggest banks. (See item 6)

- The Associated Press reports that 52 people were arrested in Florday last week on criminal and immigration charges stemming from an alleged scheme to sell commercial Florida drivers licenses which allow drivers to operate fuel tankers, hazardous material trucks and other heavy machinery. (See item 10)

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. *April 29, Courier−Journal (KY)* — **Widespread blackout unlikely in Kentucky.** A widespread electric outage like the one that left millions powerless in the Northeast in 2003 can't be ruled out in Kentucky, but the state's ability to generate plentiful amounts of electricity provides some protection against such problems, according to a Kentucky Public Service Commission (PSC) report released on Thursday, April 28. Commonwealth Associates, a Jackson, MI, engineering consulting firm prepared the report using computer simulations of nearly 100,000 scenarios that could strain the state's grid. Fewer than 1,200 of the scenarios

showed any possibility of creating widespread outages. Of those, fewer than 150 were problems that could happen under normal conditions. The rest were failures under "extreme grid−operation scenarios," the report said. The state's power companies, which paid for the study, already have been alerted to potential problem areas. "The PSC expects regulated utilities to move swiftly to deal with those weaknesses," said commission Chairman Mark David Goss.
Assessment of Kentucky’s Transmission System Vulnerability to Electrical Disturbances: http://psc.ky.gov/agencies/psc/hot_list/200500090report.pdf
Source: http://www.courier−journal.com/apps/pbcs.dll/article?AID=/20050429/BUSINESS/504290366/1003

2. *April 29, Reuters* — **Sabine Channel in Texas remains shut to tankers.** The Sabine Channel remained shut Friday, April 29, for oil tankers with efforts to salvage a sunken 101−foot crew boat under way, the U.S. Coast Guard in Houston said. The channel is used by oil tankers heading to and leaving oil refineries and chemical plants in Port Arthur and Beaumont, TX. It was shut Thursday, April 28, after a petroleum tanker collided with a crew ship. Eight vessels, some of them oil tankers, waited offshore in the Gulf of Mexico while three vessels were not able to leave the Sabine River because of the traffic restrictions, said Adam Wine of the U.S. Coast Guard. Four refineries served by tankers using the channel account for about six percent −− about 1.05 million barrels −− of the crude oil refined daily in the United States. It generally takes three to four days of the channel being shut before operations at the plants are affected, marketing sources said. There was no estimate of how long salvage will take so that tankers could pass the channel. The Sabine Channel runs from the Gulf of Mexico into the Sabine River, which forms the border between Texas and Louisiana.
Source: http://news.yahoo.com/news?tmpl=story&u=/nm/20050429/us_nm/energy_channel_texas_dc_1

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

Nothing to report.

[Return to top]

Banking and Finance Sector

3. *April 29, Sun−Sentinel (FL)* — **Florida university warns of identity theft risk after computer breach.** Some Florida International University (FIU) students, professors and staffers may be at risk of identity theft from a recent computer break−in, the university said. The university still is gauging the extent of the security breach. However, for now, there's no evidence of any fraud, FIU information−systems chief John P. McGowan said. He said

cyber−burglars recently may have peeked into 165 campus computers which held some sensitive information, such as employees' lists of their credit−card accounts, and old class rosters that could include students' Social Security numbers. FIU stopped using the Social Security numbers on class lists last year. According to McGowan, the electronic intruders apparently dialed into FIU's computers from Europe.
Source: http://www.sun−sentinel.com/news/local/palmbeach/sfl−ppfiu29 apr29,0,830444.story?coll=sfla−news−palm

4. *April 29, Government Accountability Office* — **GAO−05−368: Currency Paper Procurement: Additional Analysis Would Help Determine Whether a Second Supplier Is Needed (Report).** For over 125 years, the Bureau of Engraving and Printing (BEP), within the Department of the Treasury, has relied on a single contractor to supply the paper for U.S. currency. Such a long−term contracting relationship could contribute to higher costs and other risks. In solicitations for currency paper contracts in 1999 and 2003, BEP took steps to address barriers to competition that the Government Accountability Office (GAO) had identified in 1998 through a survey of paper manufacturers. This report updates GAO’s 1998 report using data from a second survey. It addresses (1) the changes BEP made to encourage competition and the results of its efforts, (2) the steps BEP took to ensure that it paid fair and reasonable prices, and (3) the analysis BEP has done of the advantages and disadvantages of obtaining a second supplier. GAO recommends that the Secretary of the Treasury direct the Director of BEP to (1) increase outreach to paper manufacturers before issuing solicitations and (2) assess the need for a second supplier of currency paper and if a second supplier is needed, take the necessary action to obtain one.
Highlights: http://www.gao.gov/highlights/d05368high.pdf
Source: http://www.gao.gov/new.items/d05368.pdf

5. *April 28, Consumer Affairs* — **Online banking needs stronger security.** Email−based phishing attacks are rapidly morphing into more insidious forms of online fraud, a research report warns. The report from TowerGroup, an advisory research and consulting firm, finds that advanced approaches to online fraud −− using methods like spyware, browser hijacking and remote administration tools −− pose a significant and fast−growing threat to consumer confidence in the online banking channel. In the face of this fraud evolution, the practice of requiring a username and password as the sole means of online customer authentication is rapidly becoming outdated. "The U.S. financial services industry is continuing to build effective defenses against phishing, with consumer education playing a critical role," said George Tubin, author of the research. "However, these existing defenses do little to protect financial institutions or their customers from fraud methods that don't require the consumer to manually serve up personal or account data. Because emerging fraud techniques could potentially lead to higher levels of compromised personal data, it becomes imperative for the financial services community to enhance the rigors of online security and customer authentication," Tubin said.
TowerGroup press release: http://www.towergroup.com/research/content/news_view.jsp?new sId=520
Source: http://www.consumeraffairs.com/news04/2005/online_banking.ht ml

6. *April 28, NBC News* — **Massive bank security breach uncovered in New Jersey.** In court Thursday, April 28, Orazio Lembo was described as the alleged ring leader of what police say

was a massive scheme to steal 500,000 bank accounts and personal information, then sell it to bill collectors. Lembo's alleged accomplices included branch managers and employees from some of New Jersey's biggest banks, including Bank of America, Wachovia and Commerce Bank. All of them are accused of turning over customer bank account numbers and balance information for a profit of $10 per account. "In some cases, the bank employees printed out entire customer computer screens and turned them over to Lembo," says Hackensack, NJ chief of police Charles Zisa. "That information was then sold to his clients, which included more than 40 law firms and collection agencies." Investigators say Orazio Lembo operated his company, DRL & Associates, out of his home, paying his accomplices tens of thousands of dollars over a four−year period. Security experts say the New Jersey case illustrates once again the vulnerability of private information, even when it’s supposed to be safe inside your bank. Investigators are now trying to determine how that information was used by the debt collectors and lawyers, and whether they knew it had been obtained illegally.
Source: http://www.msnbc.msn.com/id/7670774/

7. *April 28, St. Louis Post−Dispatch (MO)* — **Program targets identity thieves.** A new task force has been created in St. Louis, MO, and several other cities to tackle identity theft. The sponsor is the U.S. Postal Service, with members including the FBI, Secret Service, Social Security Administration, the St. Louis County Police Department and the banking industry. The task force wants to tackle identity theft on a regional level to catch criminals who almost never confine themselves within jurisdictional lines. Most identity−theft cases begin as a small bust by officers at a small police department. The task force then works to identify any networks. "We're trying to work up the food chain to catch the bigger cases," said U.S. Postal Inspector Dennis J. Simpson, who leads the St. Louis team. All task force members have been deputized with federal authority so they can easily move across jurisdictional lines, just as identity thieves do. Task force members say anyone who believes he or she is the victim of identity theft should call his or her police department. An officer will take a report and refer the case to the task force, if appropriate.
Source: http://www.stltoday.com/stltoday/news/stories.nsf/stlouiscitycounty/story/9B0E460086FEDBEF86256FF20012D008?OpenDocument

8. *April 27, Computing* — **UK banks may start using biometrics.** UK companies could soon have to use biometric technology to authorize major financial transactions, as part of banking industry measures to tackle Internet fraud and money laundering. The Association for Payment Clearing Services (APACS), a UK payments association, says corporate customers will be among the first to receive devices to physically confirm signatories as well as using passwords, so−called two−factor authentication. However, banks dealing with high−value electronic transactions will require more advanced security, possibly via a third means of authentication such as fingerprint or retina scanning, says Tom Salmond, a consultant for APACS' e−commerce group. “If you have multiple signatories on an account it's quite difficult to authenticate all of them, outside of giving them all different passwords,” said Salmond. “So instead there's something you have, such as a token device or chip. Then there's something you know, such as a password or PIN. Finally, there's something you are, such as a biometric. That kind of architecture would only be deployed for the really high−value payments.”
APACS: http://www.APACS.org.uk/
Source: http://www.computing.co.uk/news/1162738

[Return to top]

Transportation and Border Security Sector

9. *April 30, Associated Press* — **Border chief says southeast Arizona needs permanent checkpoints.** The head of the U.S. Border Patrol says his agency is hampered by its inability to put up permanent checkpoints in southeastern Arizona. David Aguilar told a Senate hearing on Friday, April 29, that no similar prohibition exists in other border states, but appropriations provisions have required that all checkpoints be temporary and be moved every two weeks in Arizona. Critics say permanent checkpoints that force everyone off the road disrupt trade and traffic, however, Aguilar says they have proven effective in other states.
Source: http://www.kesq.com/Global/story.asp?S=3279760

10. *April 28, Associated Press* — **Arrests made in scheme selling commercial drivers licenses.** In Florida, state and federal officials announced Thursday, April 28, the arrests of 52 people on criminal and immigration charges stemming from an alleged scheme to sell commercial Florida drivers licenses. Among those charged were three drivers license examiners −− two in Broward County and one in Miami−Dade County −− who allegedly sold fake licenses for between $100 and $200 apiece. The licenses allow drivers to operate fuel tankers, hazardous material trucks and other heavy machinery that investigators said could potentially be used by terrorists. Officials said the scheme involved "recruiters" who would charge people between $1,500 and $3,000 to connect them with examiners who would then falsely certify the individuals as U.S. citizens and issue licenses.
Source: http://www.local6.com/news/4427518/detail.html

11. *April 28, U.S. Customs and Border Protection* — **China implements container security initiative.** U.S. Customs and Border Protection (CBP) Commissioner Robert C. Bonner and Mou Xinsheng, Minister of the General Administration of Customs of the People's Republic of China, on Thursday, April 28, announced the port of Shanghai to be the 36th operational port to target and pre−screen cargo containers destined for U.S. ports. President George W. Bush and former President Jiang Zemin reached a consensus in Crawford, TX, on October 25, 2002, to join the Container Security Initiative (CSI) in principle. "CSI is critical to securing global trade against terrorist exploitation. The CSI security blanket is now expanding and strengthening as it encompasses the port of Shanghai," said Commissioner Bonner. CBP will deploy a team of officers to be stationed at the port of Shanghai to target maritime containers destined for the U.S. Shanghai Customs officials, working with CBP officers, will be responsible for screening any containers identified as a potential terrorist risk. Under CSI, CBP has entered into bilateral partnerships to identify high−risk cargo containers and to pre−screen them before they are loaded on vessels destined for the United States. Currently, governments representing a total of 21 administrations have committed to join CSI and are at various stages of implementation.
Source: http://cbp.gov/xp/cgov/newsroom/press_releases/04282005.xml

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

12. *April 29, South Dakota Ag Connection* — **Positive test results in latest round of chronic wasting disease testing in South Dakota.** Testing for chronic wasting disease (CWD) found no substantial increase in the number of infected deer and elk in a targeted area of western South Dakota. While that's good news, the results are puzzling in some respects, said Steve Griffin, a wildlife biologist for the state Department of Game, Fish and Parks. "It's not consistent where we're finding it," he said of the 10 cases confirmed since last July. "Last year we didn't find it on the prairie, and this year we did. Two years ago we had it on the prairie, too, so we skipped a year of not finding it," Griffin said. "It's the same for the Hills. I can't explain why that's happening −− if we're getting more samples in an area from one year and not as many the next." The 10 CWD cases since last July were found in 2,693 samples collected from 701 elk, 752 mule deer, and 1,240 white−tailed deer in the Black Hills, part of Pennington County and Fall River and Custer counties. Results on three samples are pending, Griffin said. There were 14 CWD cases in 2,150 samples taken two years ago and seven positives from 2,498 samples last year.
Source: http://www.southdakotaagconnection.com/story−state.cfm?Id=34 1&yr=2005

[Return to top]

Food Sector

13. *April 29, Kansas Department of Agriculture* — **Study quantifies bovine spongiform encephalopathy cost to the U.S.** The Kansas Department of Agriculture and K−State Research and Extension Friday, April 29, released "The Economic Impact of BSE (bovine spongiform encephalopathy) on the U.S. Beef Industry," which provides a comprehensive assessment of the economic impact of lost export markets and policy changes affecting cattle procurement and processing. "The most significant economic impact of BSE is from lost beef export markets," said Kansas Secretary of Agriculture Adrian Polansky. "Alone, they accounted for a $3.2 to $4.7 billion revenue loss to the U.S. beef industry last year." Within days of the U.S. Department of Agriculture’s (USDA) 2003 announcement that a cow in Washington state had been diagnosed with BSE, 53 countries banned imports of U.S. cattle and beef. The report evaluates the potential impact BSE testing could have if it were used to regain export markets. The study also examined potential costs related to feed regulations being considered by the Food and Drug Administration. Also examined in the study was the economic impact of USDA’s rule that prohibits non−ambulatory cattle from entering the food supply.
BSE Report: http://www.accesskansas.org/kda/News/newsre/BSEStudy.pdf.
Source: http://www.ksda.gov/default.aspx?tabid=349&view=show&pressid =41

14. *April 29, Food Safety and Inspection Service* — **Ham products recalled.** Field Packing Company, an Owensboro, KY, firm, is voluntarily recalling approximately 29,000 pounds of ham products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Friday, April 29. The hams

were were distributed to institutional and food service customers in California, Indiana, Kentucky, Missouri, and Minnesota. The hams were also distributed to retail stores in Illinois, Indiana, Kentucky, Missouri, and Tennessee. The problem was discovered through company testing. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_024_2005_Relea se/index.asp

15. *April 28, District of Columbia Department of Health* — **Health advisory on lead in candy imported from Mexico.** Gregg A. Pane, Director of the District of Columbia Department of Health (DOH), Thursday, April 28, issued a health advisory that lead has been found in products imported from Mexico and marketed as food seasonings, but consumed by children as candy. Several of the lead−tainted products are produced by Lucas candies, a subsidiary of candy maker Mars, Inc. Representatives from Mars have stated that they no longer make these products and are committed to getting remaining supplies off of the shelves. The DOH is working cooperatively with federal agencies to address this issue and reduce the risk of lead exposure through joint inspections and investigations.
Source: http://dchealth.dc.gov/news_room/release.asp?id=290&mon=2005 04

16. *April 28, Food Safety and Inspection Service* — **Chicken wraps recalled.** Forest and Brook Food Corp., a Hauppauge, NY, establishment, is voluntarily recalling approximately 385 pounds of chicken breast wrap sandwiches that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Thursday, April 28. The products were were distributed to retail establishments in New York, New Jersey, and eastern Pennsylvania. The problem was discovered through company testing. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_023_2005_Relea se/index.asp

[Return to top]

Water Sector

17. *April 28, Barrington Times (RI)* — **Rhode Island boil−water order crisis continues.** An East Providence, RI, boil−water advisory continued last week and will last through Wednesday, May 4, as the Department of Health works with town officials to locate the source of two positive E. coli tests dating back to Saturday, April 16. The recent bacteria contamination is the second this year. The first incident was in January, but an initial test was misread, leading town officials to discover the contamination long after the fact. A bill sponsored by East Providence legislators was close to passage when the April contamination was found. The bill states that all water test results must be passed on to the director of Rhode Island's Department of Health for a second review.
Source: http://www.eastbayri.com/story/283178667292268.php

[Return to top]

Public Health Sector

18. *April 29, Associated Press* — **Numbers up in Florida for parasitic illness.** At least 30 people have gotten sick in Florida in recent weeks from a parasite that can spread illness through contaminated food or water. State health officials usually see only a few cyclospora illnesses each year. The recent spike suggests a shared source, but investigators have not tracked it down. "We are looking to identify any potential links that these cases have," Lindsay Hodges, a spokesperson for the state Health Department, said Thursday, April 28. Cyclospora are microscopic, one−celled organisms that can contaminate fresh produce and burrow in the small intestine. The Health Department issued an alert to physicians and health care providers, telling them to consider cyclospora as a diagnosis.
Source: http://www.macon.com/mld/macon/news/nation/11520835.htm

19. *April 29, Reuters* — **Major polio epidemic hits Yemen.** A polio epidemic has infected 22 children in Yemen, and the virus is threatening to spread further, the World Health Organization (WHO) said on Friday, April 29. The WHO, which reported four cases around the Red Sea port city of al−Hudaydah last week, said 18 more children had contracted the disease in the Arab state. It is the latest setback to the WHO's campaign to wipe out transmission of polio worldwide by year−end. An epidemic which originated in Nigeria has swept across Africa since mid−2003. "What we are facing now is a major epidemic of polio in Yemen," David Heymann, head of the WHO's polio eradication program, told a news briefing. "Experts fear that the number of cases will rise in the immediate future," the WHO said in a statement. It said it was investigating other suspected cases, and low immunization rates among Yemeni children could facilitate the outbreak's spread. The WHO was awaiting genetic analysis of the virus to determine whether it had come from neighboring Saudi Arabia or Sudan, which have both registered cases in the past year.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=worldNews&storyID=2005−04−29T125331Z_01_HOL946388_RTRUKOC_0_YEMEN−POLIO.xml

20. *April 29, PharmaLive* — **Vaccine provides full protection against Ebola according to results of animal studies.** Dutch biotechnology company Crucell N.V. Friday, April 29, reported new results from its Ebola vaccine studies. The studies, conducted together with the Vaccine Research Center (VRC) of the U.S. National Institutes of Health (NIH) and the U.S. Army Research Institute of Infectious Diseases (USAMRIID), confirm previously published results showing that a single shot of the vaccine protected monkeys completely against Ebola. The results of the studies were detailed by Nancy Sullivan, head of the VRC's Biodefense Research Section, at a scientific meeting held Thursday, April 28, at USAMRIID in Fort Detrick, MD.
Source: http://www.medadnews.com/News/Index.cfm?articleid=234467

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

21. *April 29, News Tribune (IL)* — **Homeland security drill tests response time, cooperation of agencies.** The village of Hennepin, IL, served as a host Thursday April 28, to a homeland security preparedness exercise that involved numerous local, state, and federal agencies. The Illinois Army National Guard, in coordination with the U.S. Coast Guard, Federal Bureau of Investigation, Illinois Emergency Management Agency, Putnam County Sheriff’s Department, and Hennepin fire, police, and ambulance services, conducted the drill. The purpose of the drill was to practice identifying, locating, and responding to a transportation−related security threat. In the scenario set up for the drill, members of the National Guard 5th Civil Support Team based out of Bartonville had to enter a barge on the riverfront to respond to reports of a potential chemical agent or weapons of mass destruction there. “We wanted to have a challenging marine incident,” said Joe Snowden, a lieutenant commander with the U.S. Coast Guard. The drill tested how well the different agencies were able to work together, as well as their response time to the emergency situation.
Source: http://www.newstrib.com/main.asp?FromHome=1&TypeID=1&ArticleID=16785&SectionID=1&SubSectionID=207

22. *April 29, U.S. Geological Survey* — **U.S. Geological Survey report details preparedness for a volcanic eruption.** A National Volcano Early Warning System (NVEWS) is being formulated by the Consortium of U.S. Volcano Observatories (CUSVO) to establish a proactive, fully integrated, national−scale monitoring effort that ensures the most threatening volcanoes in the U.S. are properly monitored in advance of the onset of unrest and at levels commensurate with the threats posed. Volcanic threat is a combination of hazards (the destructive natural phenomena produced by a volcano) and exposure (people and property at risk from the hazards). The U.S. has abundant volcanoes, and over the past 25 years the Nation has experienced a diverse range of the destructive phenomena that volcanoes can produce. Hazardous volcanic activity will continue to occur, and because of increasing population, increasing development, and expanding national and international air traffic over volcanic regions the exposure of human life and enterprise to volcano hazards is increasing. Fortunately, volcanoes exhibit precursory unrest that if detected and analyzed in time allows eruptions to be anticipated and communities at risk to be forewarned with reliable information in sufficient time to implement response plans and mitigation measures.
Source: http://pubs.usgs.gov/of/2005/1164/

[Return to top]

Information Technology and Telecommunications Sector

23. *April 29, FrSIRT* — **Redhat security update fixes multiple Mozilla vulnerabilities.** Redhat has released a security patch to correct various vulnerabilities in Mozilla. The vulnerabilities can be exploited by malicious people to gain knowledge of potentially sensitive information. This could allow cross−site scripting attacks, bypass certain security restrictions, and compromise a user's system. The flaws could be exploited by malicious websites to execute arbitrary commands and cause a denial of service. Use Red Hat Network to download and

update your packages: http://rhn.redhat.com/
Source: http://www.frsirt.com/english/advisories/2005/0428

24. *April 29, New York Times* — **New York sues California Internet company on use of spyware.** A broad investigation into Internet abuses led the New York attorney general to file a lawsuit on Thursday, April 28, accusing a California company of clogging computers across the nation with secretly installed spyware and adware, which can vex users and impede the flow of commerce on the Web. The attorney general, Eliot Spitzer, sued Intermix Media, a large Internet marketing firm, accusing it of embedding "several types of invasive and annoying" programs on its Web domains that can pop up, route users to unwanted sites or link them to Intermix's services and clients. In recent years, companies have tried to sneak what consumer advocates call parasitic software into computers that tracks users' browsing habits, but government inquiries into such practices have been rare, said Ben Edelman, a Harvard University researcher who studies spyware. An official with Intermix, in a statement posted on Thursday on the company's Website, said that the company neither promoted nor condoned spyware, and that many of the practices being challenged by Mr. Spitzer began under the company's previous leadership.
Source: http://www.nytimes.com/2005/04/29/nyregion/29internet.html

25. *April 28, Secunia* — **Golden FTP Server Pro Log parsing buffer overflow vulnerability.** A vulnerability exists in Golden FTP Server Pro, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the log parsing functionality when handling entries in the "gftppro.log" log file. This can be exploited to cause a stack−based buffer overflow by passing an overly long argument about 336 bytes to the "USER" FTP command when attempting to log in. There is no solution at this time.
Source: http://secunia.com/advisories/15156/

26. *April 28, InformationWeek* — **IT executives tell software vendors that software must improve.** A panel of IT execs at Sand Hill Group's Software 2005 conference in Santa Clara, CA, said Wednesday, April 27, the software industry needs to build higher−quality software and closer relationships with customers. Representing billions of dollars in annual technology spending, IT leaders from British Petroleum, Lockheed Martin, Unilever, and Kaiser Permanente made it clear that the software industry needs a new business model, better quality control, and closer product development ties with customers. Perhaps the most disturbing were the panelist's descriptions of software vendors compounding one problem with another. Neil Cameron, CIO of Unilever, which makes consumer goods, said the software the company uses to run its various business units is making what should be a simple business painfully complex −− thanks to issues such as buggy applications and the constant efforts to keep up with patch management. The panelists agreed that software security issues are taking up too much of their time and money, and that a portion of the blame for that lies with the vendors.
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=161601417

27. *April 28, IDG News Service* — **U.S. seeks greater microchip industry protection.** The migration of microchip production outside the U.S. poses a major threat to the nation's security and economy and the Department of Defense should take the lead in efforts to rebuild the industry at home, warns a recent report from a federal advisory committee. It points to China as a beneficiary of current trends. "From a U.S. national security view, the potential effects of this

restructuring are so perverse and far reaching and have such opportunities for mischief that, had the United States not significantly contributed to this migration, it would have been considered a major triumph of an adversary nation's strategy to undermine U.S. military capabilities," says the report, from the U.S. Defense Science Board Task Force on High Performance Microchip Supply, dated February 2005. The report puts renewed emphasis on a call for revitalizing U.S. chip production in the face of its continued migration overseas, and warns that losing the manufacturing end of the chip industry ultimately puts research and development at risk since, historically, "R&D tends to follow production.
Report: http://www.acq.osd.mil/dsb/reports/2005−02−HPMS_Report_Final .pdf
Source: http://www.infoworld.com/article/05/04/28/HNmicrochip_1.html

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: A remote exploitation of a buffer overflow vulnerability in Citrix Systems Inc.'s Program Neighborhood Agent allows attackers to execute arbitrary code under the privileges of the client user. The problem specifically exists in the client code responsible for handling the caching of information received from the server. The Program Neighborhood Agent caches information from published applications in the AppCache folder, located in the users profile directory.

Current Port Attacks

Top 10 Target Ports	20525 (−−−), 445 (microsoft−ds), 135 (epmap), 1026 (−−−), 6346 (gnutella−svc), 1027 (icq), 139 (netbios−ssn), 41170 (−−−), 30614 (−−−), 2234 (directplay) 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

28. *May 01, Associated Press* — **Two hundred held after attacks in Egypt.** Police on Sunday, May 1, detained about 200 people from the home villages of the three attackers responsible for

a bomb blast and tour bus shooting near Cairo tourist sites the day before, authorities said. The records of the detainees, from the villages of al−Ammar and Ezbet al−Gabalawi north of Cairo, are being examined for any connections with local terror networks, police said. On Saturday, April 30, a man identified as a suspect in an April 7 bombing blew himself up as he leapt off a bridge during a police chase, officials said. Less than two hours later, two veiled women −− reportedly the man's sister and fiancee −− attacked a tour bus. Egyptian police officials and the government−guided Al−Ahram newspaper said the bus was carrying Israeli tourists. Nine people, four of them foreigners, were wounded in the apparent revival of violence against Egypt's tourism industry. Authorities said Saturday's violence was a result of the government crackdown on a small militant cell it says carried out the April 7 suicide bombing near a Cairo tourist bazaar that killed two French tourists and an American.
Source: http://edition.cnn.com/2005/WORLD/meast/05/01/egypt.crackdow n.ap/

29. *April 30, Associated Press* — **Portland approves withdrawal from FBI−led anti−terror team.** The Portland, OR, City Council on Thursday, April 28, approved a recommendation to withdraw police officers from an FBI−led anti−terror task force after federal authorities refused to raise the mayor's security clearance to let him keep closer watch over its activities. The city is the first in the nation to pull out of the Joint Terrorism Task Force −− a network the federal agency has put together across the country. Mayor Tom Potter had felt political pressure to ensure oversight after the FBI wrongly arrested Portland attorney Brandon Mayfield as a suspect in the Madrid train bombings last year −− a mistake that prompted an FBI apology. "The FBI cannot and will not grant top secret clearances for those outside or inside the law enforcement community who do not have a direct need to know some of the country's most sensitive intelligence information," Robert Jordan, the special agent in charge of the FBI's Portland division, said in a statement last month. The mayor outlined guidelines which he said would ensure close cooperation with the FBI in anti−terror investigations, even if the officers aren't officially on the task force.
Source: http://www.pittsburghlive.com/x/tribune−review/terrorism/s_3 29612.html

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

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) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 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.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.