Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 12 April 2005

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

Daily Highlights

- USA TODAY reports the federal government is increasing its investigation of airliner maintenance−and−repair firms after six illegal immigrants allegedly used false documents to gain Federal Aviation Administration approval to work as mechanics. (See item 10)
- The Associated Press reports that Golden Gate Bridge officials are re−evaluating security after a driver was charged with attempted murder in the shooting of a toll collector Saturday. (See item 12)

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 11, Reuters* — **OPEC set to boost supplies in May.** The Organization of the Petroleum Exporting Countries (OPEC) is on track to boost supplies to world markets by 500,000 barrels per day (bpd) next month to help build stockpiles ahead of an anticipated demand surge later this year, the cartel's president said on Monday, April 11. Sheikh Ahmad al−Fahd al−Sabah, also Kuwait's oil minister, said that production from the group's 10 members bound by quotas was expected to rise to 28.5 million bpd in May from just over 28 million now. Some in OPEC, particularly Saudi Arabia and fellow Gulf producers, are keen to boost output now to encourage stock building in the coming months to avoid a potential supply crunch and price spike late this

year. The cartel expects the call on OPEC in the last three months of 2005 to swell to 30.3 million barrels per day from 28.5 million in the third quarter.
Source: http://www.washingtonpost.com/wp−dyn/articles/A42965−2005Apr 11.html

2. *April 11, Associated Press* — **Spent fuel to remain at decommissioned plant in Massachusetts.** About 1,700 tons of spent nuclear fuel will remain on the site of the decommissioned Yankee Rowe nuclear power plant for the foreseeable future even though demolition of most of the structures are scheduled to be completed on schedule by the fall, company officials say. The spent fuel will be kept on site under tight security while the controversy over a proposed federal nuclear repository at Yucca Mountain, NV, is resolved. A 90−acre section of the 1,800−acre site in Rowe will remain the home of 16 dry cask storage units containing spent nuclear fuel, officials said recently at a meeting of the Yankee Rowe Community Advisory Board. The casks contain 533 fuel assemblies −− bundles of hollow steel rods that contain ceramic−coated pellets of highly refined uranium. Yankee Rowe, located in western Massachusetts, was shut down in 1992 after 31 years of operation.
Source: http://www.thebostonchannel.com/news/4365738/detail.html?rss =bos&psp=news

[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 11, Mercury News (CA)* — **Banks fight phishing scams.** Banks are using a growing array of technologies to uncover, divert or spike e−mail scams known as phishing. Phishing costs banks, online merchants and credit card companies an estimated $350 million to $500 million a year in losses or reimbursements to defrauded customers. With the help of multiple technologies, banks are finding they can make it harder for phishers to cash in on their efforts −− either by spotting fake e−mails and preventing them from being delivered, getting fake sites shut down quickly, or using their knowledge of customer patterns to know when it's a phisher −− not a legitimate customer −− logging in to make a withdrawal. “A lot of the top banks have been putting these technologies in the background,” said George Tubin, senior analyst at TowerGroup of Needham, MA. “Now the smaller banks are doing a better job, too,” he added. Most are using more than one of several security approaches offered by security vendors.
Source: http://www.mercurynews.com/mld/mercurynews/11364930.htm

4. *April 10, Reuters* — **Banks, government team up to fight terrorism.** In the summer of 2001, before the September 11 terrorist attacks, nobody had heard of “financial tracking.” Today, this

little−publicized technique, which combines financial systems with nuggets of specific intelligence from the government, is one of the most valuable tools in the fight against terrorism financing, helping to track down militants, watch their moves and thwart attacks, officials and experts say. The process takes place behind the scenes, and while successes are real, they never make headlines because officials are afraid of endangering sources and methods. “We miss an awful lot, but there are some really stunning accomplishments by the people who work quietly in the dead of the night,” said David Aufhauser, the Department of Treasury's former general counsel who spearheaded the fight against terrorism financing after the 2001 attacks. Unlike money laundering, which often triggers red flags that banks can detect, financial institutions struggle to spot terrorist financing proactively, without government tip−offs. However, if government officials can provide a specific morsel of hard−won intelligence that goes beyond the names and aliases they routinely provide, banks' computers become a powerful search engine that can help monitor militants' activities, including where they are, what they buy and whom they know.
Source: http://www.nytimes.com/reuters/business/business−bizsecurity −banks.html

5. *April 10, Washington Post* — **Virginia lawmakers plan to catch cyberscammers.** The Virginia General Assembly this year passed a handful of new bills aimed at cracking down on computer and online crimes, including a statute that observers say is the nation's first law that criminalizes phishing schemes. Starting July 1, cyberscammers who deceive people out of personal information could face a felony charge punishable by up to five years in prison and $2,500 in fines. Those convicted of selling the data or using it to commit another crime, such as identity theft, would face twice the prison time. Other new laws boost penalties for hackers convicted of computer trespassing or invasion of privacy, which includes disabling a computer with a virus, stealing personal data directly from a computer or using spyware programs to do so. Lawmakers said the changes will give prosecutors more power to go after cybercriminals and deter others from committing high−tech crimes.
Source: http://www.washingtonpost.com/wp−dyn/articles/A40578−2005Apr 9.html

6. *April 10, Winnipeg Sun (Canada)* — **Canadian police fear theft was done for identity fraud.** Royal Canadian Mounted Police (RCMP) believe a robbery at an insurance agency may have been the first step towards stealing the identity of hundreds of individuals. Thieves who recently broke into Slater Roy Agencies in Stonewall, Manitoba, Canada, made off with computer equipment to make the photo identification portion of driver's licenses, including a camera and hundreds of blank photo identity cards. The insurance company is one of two locations in Stonewall where driver's licenses can be processed. "I would suggest the individuals who are responsible for this definitely knew what they were doing," said Stonewall RCMP Sgt. Gerry Thomas. "They had done their homework and were well−prepared."
Source: http://www.canoe.ca/NewsStand/WinnipegSun/News/2005/04/10/99 0162−sun.html

7. *April 10, Wall Street Journal* — **Authorities on the trail of identity theft rings.** Recent investigations of online identity theft rings show a disturbing pattern emerging, law enforcement officials say. Large groups of criminals are banding together to steal financial data from individuals, and then trade or sell that data on underground Internet sites. As public concern mounts about identity theft, police arrests are shedding light on the sophistication of the criminals behind such schemes. They are finding well−run, hierarchical organizations where members coordinate efforts via the Internet. Once stolen, the information is advertised and sold

on Websites and Internet chat rooms specializing in the trafficking of such valuable data. "They are run like businesses," says Larry Johnson, special agent in charge of the Secret Service's criminal investigative division. Identity theft long predates the Web, but Johnson says the Internet helps large groups communicate more efficiently and extend their geographical reach. The market for trading stolen information has grown more sophisticated in the past year, too, security experts say. Originally, large volumes of credit card or bank account information were sold indiscriminately in bulk, says John Watters, chief executive of iDefense Inc. Now, criminals are charging more if a card has a high credit limit or additional information, such as a billing address and maiden name.
Source: http://www.capecodonline.com/cctimes/biz/authoritieson10.htm

8. *April 09, Northeast Mississippi Daily Journal* — **University students left vulnerable to identity theft.** The mistake of a former employee left hundreds of University of Mississippi sorority and fraternity students vulnerable to identity theft. According to Assistant Vice Chancellor for University Relations Jeff Alford, over 300 students' names and social security numbers from 14 sororities and fraternities were placed on the university's Website. Alford said the information had probably been on the site since August 2003 when a former staff member in the Dean of Students office backed it up on the Web server to save. Alford said the former employee responsible for the leak was contacted when the school discovered the mistake. "He said he thought he had erased it and was very apologetic for the mistake," Alford said. The university shut down the site Wednesday, April 6. "The information was posted in such an obscure manor that it would have been extremely difficult for someone to access it," said Alford.
Source: http://www.djournal.com/pages/story.asp?ID=190865&pub=1&div= News

9. *April 08, AuctionBytes.com* — **E−mail feature used to target eBay sellers.** Users of eBay have long suffered scam attacks by fraudsters. One of the scams making the rounds takes advantage of eBay's "Ask Seller a Question" feature that allows potential bidders to query sellers through eBay's e−mail system. However, rather than asking a question about the item for sale, the scammer posts an advertisement for a partner to help it process PayPal payments. PayPal prohibits users from using their PayPal accounts to collect and transfer money for someone else, most often this is for money−laundering purposes. Phishing e−mails are old, but they continue to plague eBay users with new twists, including ones sent to look like they come from eBay inviting the seller to become a PowerSeller or to participate in contests. Another scam is one that takes advantage of users' desire to protect themselves from identity theft. One eBay seller reported receiving a hoax e−mail that started off, "Daily Monitoring of your visa credit card and debit is the only way to protect potential identity theft in progress. After so much identity theft in progress towards the Visa Institution we are proud to present the new Anti−Theft service called (Verified by Visa)."
Source: http://www.auctionbytes.com/cab/abn/y05/m04/i08/s01

[Return to top]

Transportation Sector

10. *April 11, USA TODAY* — **Scrutiny of airline−maintenance firms grows.** The federal government is increasing its investigation of airliner maintenance−and−repair firms after six

illegal immigrants allegedly used false documents to gain Federal Aviation Administration (FAA) approval to work as mechanics. The six are among 28 undocumented workers arrested in North Carolina during a March 8 immigration enforcement sweep at a sprawling airliner−repair facility in Greensboro owned by Timco Aviation Services. Thirteen of the 28 were indicted in federal criminal court on charges such as lying and using fake citizenship documents to get hired. The other 15 will be deported. Although the government is not alleging ties to terrorism, the ability of foreign nationals to beat safeguards and work on airliners has raised concern. FAA spokesperson Kathleen Bergen said the six who hold licenses passed FAA tests. Financially squeezed airlines are outsourcing more maintenance to cut costs, and independent contractors such as Timco are expanding. Last month, Delta said it will outsource work on 344 jets. Airliner maintenance and repair is a $37 billion industry that is benefiting as travel demand grows and airlines turn to outside companies to maintain planes more cheaply.
Source: http://www.usatoday.com/travel/news/2005−04−11−air−maintenan ce−usat_x.htm

11. *April 11, Associated Press* — **Blizzard hammers Colorado and disrupts travel.** Travelers spent Sunday night, April 10, sleeping in airport terminals and hunkered down at truck stops and churches after a howling blizzard grounded airplanes, shut down highways, and snapped tree limbs. Almost a foot of snow fell in Denver on Sunday and two feet fell in Greenland, about 20 miles north of Colorado Springs, the National Weather Service said. Snow was tapering off Monday, April 11, but still fell across the eastern part of the state and adjoining areas of western Kansas, the Nebraska Panhandle and parts of Wyoming and South Dakota. Most airlines delayed or canceled flights Sunday, including United Airlines, the biggest carrier at Denver International Airport, officials said. Flights also were canceled out of Colorado Springs. About 2,000 travelers were stranded overnight at Denver International, airport spokesperson Steve Snyder said. He said it could be Tuesday, April 12, or later before airline schedules return to normal. Interstate 70 remained closed Monday morning between suburban Aurora, CO, and Colby, KN, a stretch of about 200 miles, according to police and highway officials in both states.
Source: http://www.nytimes.com/aponline/national/AP−Colorado−Blizzar d.html?pagewanted=all&oref=login

12. *April 11, Associated Press* — **Golden Gate Bridge security re−evaluated.** Golden Gate Bridge officials are re−evaluating security after a driver was charged with attempted murder in the shooting of a toll collector. The female toll worker was shot in the neck and chest late Saturday, April 9, apparently during an attempted robbery, according to San Francisco police. She is expected to survive. It's the first time a toll collector has been shot on the bridge, said Mary Currie, spokesperson for the Golden Gate Bridge administration. The span is one of the most heavily guarded sites in the Bay Area. Currie said officials are examining the circumstances of the attack and interviewing toll collectors as they reconsider security measures.
Source: http://wireservice.wired.com/wired/story.asp?section=Breakin g&storyId=1017121&tw=wn_wire_story

13. *April 11, Associated Press* — **New York City gets high−tech subway.** This month's launch of fully automated trains on a 24−station line connecting Manhattan and Brooklyn is a big change for the New York subway. L line trains will run without conductors, except in emergencies, coasting along at preordained speeds and stopping automatically at stations, a lone train

operator in the front car watching the controls. San Francisco has had this technology for years, and Paris has one such line. But the New York City Transit upgrade is a milestone. Never has a city with a subway so large or so old −− it turned 100 last fall −− tried to convert its existing infrastructure to automation. If all goes well, automation will be phased in on other lines over the next 20 years, and conductors will be phased out. We're moving from a 19th−century subway system," said Charles Seaton, a transit spokesperson. "It's making the system more efficient, safer and allowing us to run more trains." The new technology is not without its critics, who are worried about safety.
Source: http://www.cbsnews.com/stories/2005/04/11/tech/main687248.sh tml

14. *April 07, Transportation Security Administration* — **Explosives detection trace portal deployed to Miami International Airport.** The Transportation Security Administration (TSA) announced that Miami International Airport (MIA) will receive a new explosives detection trace portal to screen passengers at the Concourse E security checkpoint, starting Thursday, April 7. Miami will be the tenth airport to participate in this pilot. The equipment is part of the Phase II pilot program to test and evaluate the trace portal for screening passengers for explosives. At Miami, some passengers will be directed by the TSA screeners to step into the trace portal. Passengers will stand still for a few seconds while several “puffs” of air are released. The portal will collect and analyze the air for traces of explosives and a computerized voice will tell passengers when to exit. Even as the pilot program continues, TSA has allocated $28.3 million to purchase and install an additional 147 trace portals. TSA is currently developing a purchase and deployment plan to have the equipment in airports by January 2006. Once the plans are finalized, TSA will announce the next group of airports to receive the equipment.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 011514b

[Return to top]

Postal and Shipping Sector

15. *April 10, WISC−TV (WI)* — **Madison post office to receive detection system.** Madison will be the second city in Wisconsin to receive a system that identifies biohazards in the mail. The U.S. Postal Service said the system will be installed and operational at the Madison area mail processing center by the end of April. The postal service said the idea behind the system is to confine a biohazard before it gets out in the general public. The biohazard detection system has the ability to find anthrax. It will be expanded in the future to detect other biohazards. Milwaukee was the first city in the state to use the biohazard detection system in its post office.
Source: http://www.channel3000.com/technology/4365396/detail.html

16. *April 09, Inside Bay Area (CA)* — **Berkeley man sentenced to two years in mail theft scheme.** A Berkeley, CA, man who was part of what prosecutors called "one of the largest and most sophisticated postal theft schemes" in San Francisco Bay Area history, has been sentenced to two years in federal prison. Moi Keopaseuth pleaded guilty to conspiracy to steal and possess U.S. mail. U.S. Attorney Kevin Ryan said Friday, April 8, that "thousands of individuals were victimized by this conspiracy to steal mail and use information from that stolen mail to obtain credit cards and steal funds from bank accounts." Prosecutors said that from 1999 until late 2002, the thieves broke into Bay Area mailboxes by force or with counterfeit postal keys. They

took the stolen mail to San Francisco, CA, and organized it to create libraries of confidential identity and financial information. They then used this stolen information to obtain credit cards and fraudulently buy goods and services. Credit card companies, banks, hotels and other businesses suffered about $500,000 in losses.
Source: http://www.insidebayarea.com/ci_2647694

[Return to top]

Agriculture Sector

17. *April 11, Associated Press* — **Sheep, insects to help eradicate exotic weeds.** Three of Arizona's national forests will soon be home to weevils, flies, moths, beetles, and sheep. They are expected to be sent in as early as this summer to ingest dangerous and invasive weeds that are harming endangered and threatened native plants and wildlife. This is part of a U.S. Forest Service plan to treat 25 species of weeds on 135,000 acres of the Coconino, Kaibab, and Prescott national forests in northern Arizona over the next 10 years. Forest officials also will be spraying, mowing, burning, hoeing, pulling, and digging to control the invasive weeds. Implementation is set for June 1. The goal is to contain or control 14 invasive species and to eradicate eight species that are threatening the biological diversity of the area. They also want to prevent new plants from becoming established. The invasive weeds pose a threat to nine plant species, seven types of fish and eight species of animals that are listed as threatened or endangered.
Source: http://www.nytimes.com/aponline/business/AP−Exotic−Weeds.htm l?

18. *April 11, USAgNet* — **Farmers' rights to apply pesticides challenged in Maine.** Threats of a lawsuit have forced a Maine blueberry grower to abandon his legal right to aerial spray. The blueberry farm was threatened with a lawsuit by activist groups unless the family farm sought Clean Water Act permits to aerially apply pesticides. The farm announced Sunday, April 10, that it would cease aerial spraying because the legal defense costs would threaten the 125−year old farm's existence. In spite of the activists' claims, for the last three decades, the Environmental Protection Agency, and now the Maine Department of Environmental Protection, have said that Clean Water Act permits are not necessary for pesticides applied in compliance with federal pesticide laws and regulations.
Source: http://www.usagnet.com/story−national.cfm?Id=379&yr=2005

19. *April 11, New York Ag Connection* — **Test results show more cases of chronic wasting disease in New York herd.** Test results from the two white−tailed deer herds confirmed positive for Chronic Wasting Disease (CWD) in Oneida, NY, that were sampled last week have revealed three additional deer infected with CWD. The New York State Veterinary Diagnostic Laboratory at Cornell University conducted the CWD tests on the twenty deer, and notified the state Department of Agriculture and Markets (DAM) of the three positive test results, Sunday, April 10. The three white−tailed deer that tested positive for CWD all came from the index herd, owned by John Palmer, who at the time had 18 deer on his premises. Although DAM is still investigating the source of the infection, the prevalence of CWD in the Palmer herd provides some indication that the disease may be a more recent infection. The prevalence may also provide clues as to the source of infection and the risk to other captive herds and the surrounding wild deer population. No additional positives were found in the two white−tailed

deer tested at the second confirmed herd.
Source: http://www.newyorkagconnection.com/story−state.cfm?Id=125&yr =2005

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

20. *April 11, Agence France Presse* — **Eritrea begins nationwide polio vaccination campaign.** Eritrea has launched a nationwide polio vaccination campaign to immunize all children under five as part of an Africa−wide operation aimed at halting the spread of the virus. The operation, which began Monday, April 11, targets 560,000 children across Eritrea, which despite having no reported polio cases since 1997 is believed to be at−risk due to recent appearances of the virus in neighboring Sudan and Ethiopia. Alarmed by the spread of wild polio apparently from an outbreak in Nigeria, the World Health Organization and health officials in 23 African nations plan major free vaccination drives to immunize 100 million children.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=2&u=/afp/20050411/hl_afp/eritreahealthpolioafrica_05041 1122206

21. *April 11, Chicago Sun−Times (IL)* — **Hospital keyboards may be home to bacteria.** Hospital computer keyboards can harbor potentially deadly germs for as long as 24 hours, a Northwestern Memorial Hospital study has found. Researchers contaminated keyboards with three types of bacteria that can cause life−threatening infections in severely ill hospital patients. These widespread bacteria generally are harmless to healthy people, although one type can cause skin rash, boils, and blisters. As hospitals switch to electronic records, computers are showing up in more places, including patient rooms. Researchers wondered whether keyboards could provide a means for spreading germs, and the answer appears to be "yes." When keyboards were deliberately contaminated, bacteria known as Vancomycin−Resistant Enterococci (VRE), and methicillin−resistant Staphylococcus aureus (MRSA) survived for at least 24 hours. When volunteers repeatedly tapped a key contaminated with MRSA, the bacteria spread to hands 92 percent of the time. The rates were 50 percent for VRE. Results from Northwestern Memorial's study were presented at a meeting in Los Angeles of the Society for Healthcare Epidemiology of America.
MRSA information: http://www.cdc.gov/ncidod/hip/ARESIST/ha_mrsa.htm
VRE information: http://www.cdc.gov/ncidod/hip/ARESIST/vre.htm
Source: http://www.suntimes.com/output/health/cst−nws−keyboard11.htm l

22. *April 11, Vietnam News Agency* — **Bird flu death in Cambodia may have been caused by ducks.** Cambodia's third bird flu death may have been caused by contact with ducks carrying the H5N1 virus, a World Health Organization (WHO) official said on April 11. An eight−year−old girl from southwestern Kampot province died last week in a Phnom Penh hospital after being infected with the virus. WHO officials are looking at the possibility of ducks being asymptomatic carriers. They said that it has been common for ducks not to show signs of the disease but still carry and spread the virus.
Source: http://www.vnagency.com.vn/NewsA.asp?LANGUAGE_ID=2&CATEGORY_ID=33&NEWS_ID=146505

23. *April 11, Reuters* — **Fear, ignorance fuel Marburg outbreak in Angola.** Fear and ignorance are fuelling an outbreak of Marburg virus in Angola, where locals are too suspicious of medics in "astronaut" suits to let them take away infected loved ones, aid workers said on Monday, April 11. Terrified residents stoned World Health Organization (WHO) workers' vehicles late last week, putting a brief halt to their operations to contain the disease in Uige province. "We no longer have people coming to the isolation ward −− people are hiding their patients at home because they're scared. That means the virus keeps on spreading in the community," Monica Castellarnau, emergency coordinator for Medecins Sans Frontieres (MSF) in Uige, told Reuters by phone. The outbreak has killed 192 of the 213 known cases. "Wherever there is (an) epidemic we are used to seeing ... hostility, sometimes from the community, because we are interfering in how they are living," said WHO country representative Fatomata Diallo. "Especially in this kind of epidemic where you have to have special clothes, like an astronaut, and come into the family to take a sick person or suspected case. When you come to take away a body, a dead body, with all this kind of clothing, sometimes it is not easy for the community to accept it," she said.
Source: http://www.reuters.co.za/locales/c_newsArticle.jsp?type=topNews&localeKey=en_ZA&storyID=8143202

[Return to top]

Government Sector

24. *April 11, CBS/Associated Press* — **Man in Capitol bomb scare caught.** On Monday, April 11, police tackled and forcibly dragged away a man dressed in black and carrying two suitcases who had stationed himself in front of the west side of the U.S. Capitol in Washington, DC. The Senate side of the building was evacuated, reports CBS News Congressional Correspondent Bob Fuss. People on the House side were told to stay away from windows facing the west front. A large area around the Capitol also was cleared, including the area where tourists line up for tours. The area, which overlooks the National Mall, including the Washington Monument, had been filled with tourists on a beautiful spring day. The midday incident −− which occurred during one of Washington's busiest tourist times, the annual flowering of the cherry blossoms −− had forced police to evacuate that side of the Capitol in fear of a possible explosion. Police, some armed with assault rifles, moved in slowly behind the man, who faced the Capitol from a plaza below its west entrance. CBS News Correspondent Jim Stewart reports that the man was Asian or Chinese and did not understand the security guards when they questioned him. There was never any actual threat.
Source: http://www.cbsnews.com/stories/2005/04/11/national/main68723 1.shtml

[Return to top]

Emergency Services Sector

25. *April 11, Federal Computer Week* — **Security funds based on risk or population?** In the next two days, House and Senate lawmakers will discuss revamped legislation focusing on distributing federal homeland security funds based on risk and threats to areas rather than on a population−based formula. Rep. Christopher Cox (R−CA), chairman of the House Homeland Security Committee, and Rep. Bennie Thompson (D−MS), the highest−ranking Democrat on the committee, plan an April 12 preview for the Faster and Smarter Funding for First Responders Act of 2005. The proposed legislation will promote state and local first responder coordination and prioritize homeland security grants by risk. It will be followed by a hearing held by the committee's Emergency Preparedness, Science, and Technology Subcommittee on the need for grant reform for first responders. Department of Homeland Security officials say they've earmarked at least $13 billion to state and local governments to help provide training, exercises and equipment to emergency responders. One of the top concerns among state and local government officials is the need for interoperable communications equipment and the need to develop intelligence centers to collect, analyze and share information with federal officials. The substitute bill, committee aides said, would provide every state with a minimum of guaranteed funding, but on a sliding scale.
Source: http://www.fcw.com/article88558−04−11−05−Web

[Return to top]

Information Technology and Telecommunications Sector

26. *April 11, Networking Pipeline* — **VoIP security chief warns of increased security threats.** VoIP Security Alliance Chairman, David Endler, says that threats to VoIP are increasing; and emergency services, fire, and police may be targeted. The Voice Over IP Security Alliance (VOIPSA) is the first industry−wide organization devoted to promoting VoIP security. “As VoIP increases in popularity and number of deployments, so will its attractiveness to potential attackers,” Endler observes. “VoIP networks inherit most of the same security threats that traditional data networks have today,” he notes. "However, by adding new VoIP components to an existing data infrastructure, new security requirements are also added: quality of service, reliability, and privacy. We can expect to see over the next year or two VoIP specific attacks emerge that go beyond today's more prevalent data network vulnerabilities." Our reliance on voice communications for basic needs raises the stakes even higher, when you look at emergency services call centers like 911, police and fire departments, Endler says. One of the problems, he says is that “the threats have not been well identified and laid out yet in a coherent manner. That's one of the things VOIPSA is trying to change with one of our first short−term projects, the VoIP Security Threat Taxonomy.”
VOIPSA Website: http://www.voipsa.org/
Source: http://www.networkingpipeline.com/showArticle.jhtml?articleI D=160700231

27. *April 08, SecurityFocus* — **Microsoft Windows DNS resource record cache corruption**

vulnerability. A vulnerability has been discovered in the DNS server on the Windows NT and Windows 2000 operating systems. The problem occurs in the caching of glue records. It has been reported that glue records received from non−delegated name servers will be cached by default. This may allow for a malicious server to respond to a legitimate DNS query with a spoofed DNS response, designed to contain the necessary glue record characteristics.
Solution available at: http://support.microsoft.com/kb/241352/EN−US/
Source: http://www.securityfocus.com/bid/6791/discussion/

28. *April 08, San Diego Union−Tribune* — **Cingular customers in San Diego County experience intermittent service outage.** Cingular Wireless customers throughout San Diego County had trouble making and receiving calls intermittently for about four hours Thursday, April 7, when the wireless company experienced a widespread outage in the region. The problems on the network were caused when a key fiber−optic cable failed and an emergency system didn't work properly. Company spokesperson Art Navarro said that when the cable failed, it caused the network to switch to a protected stand−by mode, Navarro said. "But that stand−by side wasn't provisioned correctly so it resulted in a loss of signal," he said. Michael Shames, executive director of the Utility Consumers' Action Network, a San Diego nonprofit organization that deals with energy, utilities and telecommunications issues, said Cingular is either the largest or second largest cell phone company in San Diego County.
Source: http://www.signonsandiego.com/uniontrib/20050408/news_1b8cin gular.html

29. *April 07, Miami Herald* — **U.S. officials warn of Chinese intelligence and cyberwarfare roles in Latin America.** U.S. officials said Wednesday, April 6, there is no evidence that China is seeking to boost its military presence in Latin America, but for the first time warned about Chinese intentions to establish an intelligence and cyberwarfare beachhead in the region. Roger Noriega, assistant secretary of state for Latin America, and Rogelio Pardo−Maurer, the top Defense Department official for the Western Hemisphere, testified before a House panel as several legislators argued that China is trying to fill the void left by the lack of U.S. involvement in the region. Noriega and Pardo−Maurer said China's interests in Latin America were mostly on the economic side, but warned that Beijing could also have an intelligence agenda as it increased trade with Latin America. Pardo−Maurer said that “we need to be alert to rapidly advancing Chinese capabilities, particularly in the fields of intelligence, communications and cyberwarfare, and their possible application in the region.” This is the first time that a senior Pentagon official warned so directly about Chinese cyberwarfare capabilities in the region.
Source: http://www.miami.com/mld/miamiherald/11332057.htm

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: US−CERT is aware of multiple

vulnerabilities that exist within the Groove Virtual Office application suite. Federal Civilian Agencies that utilize this application are encouraged to take actions to minimize the exposure of these systems within their network .

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 20525 (−−−), 135 (epmap), 1433 (ms−sql−s), 6346 (gnutella−svc), 28755 (−−−), 139 (netbios−ssn), 80 (www), 5848 (−−−), 1025 (−−−) 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

Nothing to report.
[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 and assessment 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