Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 15 April 2005

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

Daily Highlights

- The Department of Homeland Security has announced a $17.1 million award to the Port Authority of New York/New Jersey and to the Ports of Los Angeles/Long Beach and Seattle/Tacoma to strengthen the security of container cargo moving through three of the nation's largest load centers. (See item 9)
- The Department of Agriculture has announced the availability of model food security plans and training that meat, poultry, and egg processing plants can utilize to strengthen security measures and prevent potential acts of intentional contamination. (See item 13)

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 14, San Diego Union−Tribune* — **Disaster drill tests readiness of nuclear plant.** Emergency planning officials staged a disaster drill with a mock helicopter crash and more at the San Onofre Nuclear Generating Station, located in San Clemente, CA, on Wednesday, April 13. Emergency personnel from various city, county, state and federal agencies responded to simulated incidents at and around the plant that gradually worsened over a five−hour period. The drill began at 8 a.m., with participants pretending that displays in the plant's control room had gone out. Crews next pretended that a Coast Guard helicopter had crashed into a plant

switchyard. Then came mock reports of a landslide, a structure fire and a fatal traffic accident near Interstate 5. There were even mock news conferences 20 miles north in Irvine, where employees of Southern California Edison, the plant's majority owner, posed as reporters asking questions of 15 emergency officials. When the drill ended around 1 p.m., coordinators called it an effective tool to get ready for any nuclear emergency at the San Onofre Nuclear Generating Station. "It's a good training mechanism," said Richard Echavarria, a Federal Emergency Management Agency specialist and operations chief for the exercises.
Source: http://www.signonsandiego.com/news/northcounty/20050414−9999−1mc14onofre.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

2. *April 14, Associated Press* — **Department of Justice wants information on acquisition.** United Defense Industries Inc. (UDI) on Thursday, April 14, said that together with BAE Systems North America Inc. it received a request from the Department of Justice (DOJ) for additional information in connection with BAE's pending acquisition of United Defense. Both companies plan to address the request promptly. British defense contractor BAE in March agreed to buy rival UDI for nearly $4 billion. The companies continue to expect the acquisition to be completed by midyear.
Source: http://biz.yahoo.com/ap/050414/united_defense_bae.html?.v=1

3. *April 14, Government Accountability Office* — **GAO−05−436T: Air Force Procurement: Protests Challenging Role of Biased Official Sustained (Testimony).** Darlene Druyun, a former high−ranking Air Force procurement official convicted of violating a conflict of interest statute, admitted to bias in favor of The Boeing Company on various procurements. The Government Accountability Office (GAO) subsequently received protests from other firms challenging the alleged improper influence of Druyun regarding contracts awarded by the Air Force under the small diameter bomb program and the C−130 avionics modernization upgrade program. The Competition in Contracting Act of 1984 provides statutory authority for GAO's bid protest function. Consistent with standard practices, GAO reviewed all available documentation, held hearings to receive testimony from witnesses, considered arguments from all interested parties, and issued decisions on each of the protests. GAO recommended that the Air Force recompete the installation phase of the C−130 contract. GAO also recommended that the Air Force conduct a thorough analysis of the possibility of recompeting the entire contract effort. As to the small diameter bomb, GAO recommended that the Air Force conduct a competitive procurement for its moving target requirement.
Highlights: http://www.gao.gov/highlights/d05436thigh.pdf
Source: http://www.gao.gov/new.items/d05436t.pdf

[Return to top]

Banking and Finance Sector

4. *April 14, Dow Jones Newswires* — **Security breach hits HSBC's MasterCard credit cards.** British financial giant HSBC PLC is notifying at least 180,000 of its customers in the U.S. who use MasterCard credit cards to make purchases that criminals may have obtained access to their credit−card information, and that they should replace their cards. The situation involves a General Motors Corp. (GM)−branded MasterCard that is one of the most widely held credit cards in the U.S. Although HSBC so far appears to be the only financial institution to disclose that it is alerting cardholders of the incident, credit cards issued by other banks also could be vulnerable. Under current rules, however, banks aren't necessarily required to alert their cardholders to the potential fraud. In a statement, Visa USA Inc. said it was aware of a "data security breach" and is "working with the merchant, law enforcement and the affected member financial institutions to monitor and prevent card−related fraud." HSBC bank manages six million GM−MasterCard branded cards in circulation.
Source: http://money.cnn.com/services/tickerheadlines/for5/200504140034DOWJONESDJONLINE000008_FORTUNE5.htm

5. *April 13, Department of Treasury* — **Al−Zarqawi financier designated.** The U.S. Department of the Treasury on Wednesday, April 13, designated Bilal Mansur Al−Hiyari for providing financial support to the Zarqawi Network, an al Qaeda−affiliated terrorist group active in the insurgency in Iraq. "By designating financiers like Al−Hiyari, we're making it harder and riskier for the Zarqawi Network to raise and move money in support of its brutal attacks against U.S. troops, coalition partners and the Iraqi people," said Robert Werner, Director of the Treasury's Office of Foreign Assets Control (OFAC). "Today's action is the third in a series of strikes by the U.S. Government to undercut the financial foundations of the Zarqawi Network." The U.S. and Iraq are submitting Al−Hiyari to the United Nations 1267 Committee, which will consider adding him to the consolidated list of terrorists tied to al Qaeda, Osama Bin Laden, and the Taliban.
Source: http://www.treasury.gov/press/releases/js2370.htm

6. *April 12, Techworld* — **Secure Sockets Layer security aiding online fraud.** The number of lower−security Secure Sockets Layer (SSL) certificates is increasing at twice the rate of the more secure organization−validated certificates −− a situation some industry observers say could lead to increased online fraud. Domain−validated certificates, a lower−assurance form of certificate that many Certification Authorities (CAs) have begun issuing relatively recently, are one of several emerging controversies affecting Internet security and e−commerce. For example, security experts recently warned that support for International Domain Names (IDNs) could lead to the counterfeiting of legitimate Websites, including the sites' SSL certificates, leading browser makers to modify the way they handle IDNs. A quarter of the SSL certificates in use are now domain−validated, according to security company Netcraft, and over the last six months their numbers grew at twice the rate of organization−validated certificates. Domain−validated certificates guarantee only that the issuer of the certificate legitimately owns the domain name, and do not address whether any business operating out of the site is legitimate. The certificates cost less than high−assurance certificates but appear the same to users, usually causing browsers to display the familiar padlock.

Source: http://www.techworld.com/security/news/index.cfm?NewsID=3468

[Return to top]

Transportation Sector

7. *April 14, Department of Transportation* — **United States, India sign Open Skies aviation agreement.** More flights, lower fares, and stronger economic ties will be the result of a new Open Skies aviation agreement between India and the United States, U.S. Department of Transportation Secretary Norman Y. Mineta said Thursday, April 14, during a signing ceremony with Indian Civil Aviation Minister Praful Patel in the Indian capital of New Delhi. The agreement is already resulting in increased air services between the two countries, the Secretary added. Delta Air Lines has announced new daily service between New York and Chennai while Northwest Airlines plans new flights between Minneapolis and Bangalore. More recently, Continental Airlines announced a new flight between Newark and New Delhi that will be the first regularly scheduled nonstop service between the U.S. and India. The Secretary also said he expects Indian carriers to follow soon with new service between the two nations. The Open Skies agreement provides for open routes, capacity, frequencies, designations, and pricing, as well as opportunities for cooperative marketing arrangements, including bilateral code sharing with domestic Indian carriers. The deal also allows all−cargo carriers to operate in either country without directly connecting to their homeland.
   See related story on the Aviation Cooperation Program:
   http://www.dot.gov/affairs/dot61−05.htm
   Source: http://www.dot.gov/affairs/dot6005.htm

8. *April 14, Department of Transportation* — **Passenger rail investment reform act introduced in Congress.** The Passenger Rail Investment Reform Act makes key reforms to transition Amtrak into a purely operating company, create a federal−state partnership to support passenger rail, introduce market−based competition to the system, and set up an inter−state compact to maintain the heavily used Northeast Corridor service. Under the legislation, Amtrak will no longer carry the burden of maintaining tracks, stations and other infrastructure. Amtrak will have the ability to be an operating company, focused solely on running trains safely and on time. Regional, state or local authorities will be empowered to make decisions about service, planning where it is and what best meets local transportation needs; as well as ensure rail operators are providing a reliable, efficient and cost effective service. The reform proposal includes a new federal−state partnership to fund capital improvements, much like the successful programs relied on in other modes of transportation, such as mass transit. The federal government will offer 50−50 matching grants to states for development of infrastructure projects that improve passenger rail service.
   Source: http://www.dot.gov/affairs/dot6205.htm

9. *April 14, Department of Homeland Security* — **Operation Safe Commerce container cargo security program funded.** The Department of Homeland Security (DHS) announced on Thursday, April 14, a $17.1 million award to the Port Authority of New York/New Jersey and to the Ports of Los Angeles/Long Beach and Seattle/Tacoma to strengthen the security of container cargo moving through three of the nation's largest load centers. These grants were awarded under the third phase of Operation Safe Commerce, a program through which ports,

federal, state, and local governments, and private businesses work together to identify, test, and share information about commercially available technologies and best business practices to improve the security of the supply chain. Operation Safe Commerce is administered by the DHS's Office of State and Local Government Coordination and Preparedness (SLGCP) in cooperation with an inter−agency steering committee, which ensures that grant funds are used to address priority vulnerabilities and support the results of testing conducted during the different phases of the program. SLGCP is DHS's primary source of assistance for state, local, and collaborative initiatives to improve the nation's ability to prevent, prepare for, and respond to terrorism.
Source: http://www.dhs.gov/dhspublic/display?content=4459

10. *April 14, USA TODAY* — **Airplanes likely to remain packed through summer.** The flights of big domestic airlines were fuller last month than in any March in history, and this is likely to continue. Easter travel and spring break last month helped the six big traditional airlines fill 82% of seats, up from 78% a year earlier, according to data tracker Back Aviation Solutions. The airlines over the period increased seats for sale by 7%. Financially ailing big carriers have pushed to sell more seats on each flight to maximize cash while controlling expenses. Sky−high fuel costs have made it more important for airlines to make the most of every flight. Rock−bottom fares have boosted already−high demand for air travel, adding more people to the typical flight. The packed flights would be encouraging for the major carriers if they were selling seats profitably. But the domestic industry has lost more than $30 billion over four years, and major airlines are poised to report big losses for the January−March quarter.
Source: http://www.usatoday.com/travel/news/2005−04−13−full−flights_x.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

11. *April 14, Agricultural Research Service* — **Efforts to solve mealybug problem.** Agricultural Research Service (ARS) scientists and cooperators have joined forces to control the pink hibiscus mealybug (PHM), which, if unchecked, could cause an estimated $750 million in crop losses annually in the U.S. This invasive pest, Maconellicoccus hirsutus, was first found in Florida several years ago and is spreading within Florida and to other states. As it feeds, the mealybug injects saliva into the plant, causing malformation, stunting and eventual death. Research leader David Hall and entomologist Stephen Lapointe of the ARS Subtropical Insects Research Unit are leading an effort to find biological methods to stop the pest. Before the pest came to Florida in 2002, Lapointe developed a simple diet for feeding the mealybugs, showing that PHM could be reared −− for research purposes −− on an artificial diet. The artificial PHM diet will enable the production of larger numbers of healthy mealybugs to rear wasps and ladybugs needed for successful PHM−control programs. The Animal and Plant Health Inspection Service and the Florida Department of Agriculture responded to the Florida

infestation by releasing two mealybug parasites, Anagyrus kamali and Gyranusoidea indica, along with a predatory ladybug. These releases have resulted in a reduction of more than 98 percent in PHM population density in some locations.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

12. *April 13, New York Department of Agriculture & Markets* — **New York to test for chronic wasting disease in wild deer.** The New York State Department of Environmental Conservation (DEC) Wednesday, April 13, announced it will sample approximately 20 wild deer in the Town of Arietta, Hamilton County in order to test for chronic wasting disease (CWD). Recently, CWD was found in two captive white−tailed deer herds in Oneida County, marking the first incidents of CWD in New York State. The State Department of Agriculture and Markets (DAM) completed testing for CWD on the two herds in an effort to control the possible spread of the disease in New York State. Five of the 22 deer from the two captive herds tested positive for CWD. DAM has been investigating other captive deer herds associated with the index herds. One of those herds that supplied deer in the mid−1990s to the index herd in Oneida County was located in the Town of Arietta in Hamilton County. Since the herd no longer exists and the owner of the herd is now deceased, DEC will sample approximately 20 wild deer in the area surrounding the former captive herd to determine if there is any reason to believe the former captive herd may have been infected with CWD.
Source: http://www.agmkt.state.ny.us/AD/release.asp?ReleaseID=1427

[Return to top]

Food Sector

13. *April 14, U.S. Department of Agriculture* — **Model food security plans for federal establishments.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Thursday, April 14, announced the availability of model food security plans and training that meat, poultry, and egg processing plants can utilize to strengthen security measures and prevent potential acts of intentional contamination. The security of meat, poultry and egg processing facilities can be enhanced through the implementation of risk−management techniques tailored to each establishment's needs. Food security plans are valuable technical and operational resources that can help plant operators identify various types of preventive steps to minimize the risk of food product tampering or other criminal actions. The model food security plans are being issued in the form of guidance documents and are voluntary. However, USDA strongly encourages all establishments operating under federal and state inspection programs to develop plans to fit their particular needs, as each plant may be vulnerable. To assist the industry in developing food security plans, Food Safety and Inspection Service (FSIS) will conduct a series of training workshops throughout the nation in May, June, and July 2005.
The model plans are available on the FSIS Website at: http://www.fsis.usda.gov.
Source: http://www.usda.gov/wps/portal/usdahome?contentidonly=true&contentid=2005/04/0127.xml

14. *April 13, Florida Department of Agriculture and Consumer Services* — **Florida fish company distributed seafood that poses potential health risk.** Florida Agriculture and Consumer Services Commissioner Charles H. Bronson announced Wednesday, April 13, that SeaSpecialties, Inc., doing business as Florida Smoked Fish Company, may have distributed

ready−to−eat smoked salmon and other seafood specialty items that are adulterated with Listeria monocytogenes. Listeria is an organism that can cause serious and sometimes fatal infections in young children, frail or elderly people, persons with weakened immune systems, and pregnant women. No illnesses have been reported to date in connection with this problem. Florida Smoked Fish Company products have been distributed to wholesalers, retailers, restaurants, and cruise ships. The contamination was noted after testing by Florida Smoked Fish Company and the Florida Department of Agriculture and Consumer Services revealed the presence of Listeria monocytogenes in multiple products produced on multiple dates by Florida Smoked Fish Company. Production of all products has been suspended while the company continues its investigation of the source of the problem and conducts in−depth cleaning and sanitizing.
Source: http://www.doacs.state.fl.us/press/2005/04132005.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

15. *April 14, Reuters* — **Angola targets risky funeral rites in Marburg fight.** Persuading Angolans to alter traditional rituals to prepare the dead for burial is one of the biggest challenges to the country's bid to stamp out the world's worst outbreak of the Marburg virus. In a country with a tradition of embracing and kissing the dead in a final farewell, it is hard to convince people that handling corpses can spread a disease that has already killed more than 200 people since last October. Most Angolan families regard kissing and embracing the body of a dead relative as an important funeral rite. Experts say protection is essential when dealing with corpses. Bodily fluid secretions increase after death, meaning the corpses of Marburg victims are highly contagious. Simply touching an infected corpse can lead to infection. A series of radio and TV advertisements being broadcast on national media both in Portuguese and eight of the most widely spoken local languages aims to educate people to help halt the epidemic. But officials say overcoming deep−rooted community traditions remains the most difficult aspect of the campaign.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=8181352

16. *April 14, Reuters* — **Vietnam finds HIV carrier infected with bird flu.** A 21−year−old woman has been infected by both the HIV virus and bird flu, the first such case in Vietnam, health officials said on Thursday, April 14. Nguyen Van Thich, head of the Center for Preventive Medicine in the northern province of Quang Ninh, said the woman, the first to be diagnosed with both bird flu and HIV in Vietnam, used to work at a hairdressor's shop. Quang Ninh province bordering China has one of the highest number of HIV carriers in Vietnam, most of them drug addicts and prostitutes. Nguyen Tran Hien, director of the National Institute of Hygiene and Epidemiology, was quoted on Thursday, April 14, by state media as saying Vietnam has taken nearly 1,000 blood samples from the patients, birds, and water fowl infected

by bird flu to help identify the map of the virus allocation. Hien said the H5N1 virus tested this year showed it has changed slightly from the type that struck in 2004, its virulence was less but the speed of its spread was higher.
Source: http://www.reuters.com/newsArticle.jhtml?storyID=8175832&typ e=worldNews

17. *April 14, Evening Standard (UK)* — **Ricin may still be at large in the UK.** An al Qaeda cell in London, England, could still have the poison ricin, police said Thursday, April 14. An al Qaeda suspect told officials that he and police killer Kamel Bourgass made two batches of ricin. The highly toxic substance has never been found. Ricin is 6,000 times more poisonous than cyanide and an amount equivalent to a grain of salt is enough to kill an adult. Bourgass, 31, was jailed Wednesday, April 13, for 17 years for a plot to kill civilians with home made poisons and explosives. The Algerian was previously jailed for life for murdering a Special Branch detective. The information that Bourgass's cell made ricin from castor beans was given to Algerian interrogators by al Qaeda suspect Mohamed Meguerba. It was his evidence that led Scotland Yard's Anti−Terrorist Branch to the flat in Wood Green where officers uncovered ingredients and equipment to manufacture a range of poisons and gases. The cell planned to put ricin on door handles of cars and shops, and open packs of toothbrushes in supermarkets and smear them with it. Officers also found recipes and plans for gases and explosives. There was evidence of a plot for a cyanide attack on the subway.
Source: http://www.thisislondon.com/news/articles/17924441?source=Ev ening%20Standard&ct=5

18. *April 13, Agence France Presse* — **Nigerian airport offers polio vaccine to arriving children.** Nigerian health officials offered polio vaccines to children under five arriving at Lagos' domestic and international airports during a four−day immunization drive, Unicef said. Nigeria is home to almost two−thirds of the cases of polio in the world −− 788 infants were paralysed by the crippling disease last year, more than twice as many as in 2003 −− and the main target for a global eradication campaign. Between Friday, April 8, and Tuesday, April 12, Nigerian health officials and colleagues from UN health agencies carried out a huge outreach program in an attempt to protect tens of millions of children around the country. And anyone arriving from abroad was offered a chance to take part. "The National Program of Immunization decided to innovate in putting vaccination points at all border posts, including at the airports, in order to immunize children coming in and going out," said UNICEF's Christine Jaulmes.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=15 07&e=11&u=/afp/20050413/hl_afp/nigeriahealthpolioaviation_05 0413124354

19. *April 12, Louisiana Department of Health and Hospitals* — **Louisiana trains neighboring states on strategic national stockpile readiness.** The Louisiana Department of Health and Hospitals, Office of Public Health's Emergency Preparedness and Response Unit in Baton Rouge hosted a three−day training program this week to help other states to become more prepared to distribute medications and medical supplies in the event of a health threat. The Centers for Disease Control and Prevention (CDC) asked Louisiana to conduct training because the state's health and emergency response workers demonstrated preparedness to respond to a health threat and distribute the Strategic National Stockpile during a drill last year. The Strategic National Stockpile is a supply of medications and medical provisions held by the CDC that can be shipped to the states in the event of a massive medical crisis. Each state must

have plans to receive and distribute medicine and medical supplies from the Strategic National Stockpile to their local communities as quickly as possible. Louisiana was one of only three states to receive the CDC's highest rating, "green," for emergency readiness after demonstrating Louisiana's ability to receive, distribute, and dispense the medications contained within the Strategic National Stockpile during a drill in March 2004.
Source: http://www.dhh.state.la.us/news.asp?Detail=494

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

20. *April 13, Iowa State Daily* — **Iowa campus hosts area exercise to simulate terrorist attack.** Dozens of law enforcement, medical assistance and state agency officials from Ames, Iowa State and surrounding counties responded to a simulated terrorist bombing and train derailment on the ISU campus Tuesday, April 12. This is the first time Ames has conducted an exercise on such a large scale, as it brought together representatives from various agencies in 16 of Iowa's 99 counties, said Bob Kindred, Ames assistant city manager. The exercise was also the first time Ames and the university have used a joint Emergency Operations Center to coordinate all activities among the various departments and agencies involved in responding to a terrorist attack, Kindred said. Rather than conduct a similar exercise where officials respond to a mock situation by going out into the field, Kerns said it was important that Tuesday's exercise test department's ability to orchestrate, plan and communicate activities in times of emergency. "This test validates emergency procedures and lets decision−makers become comfortable with each other, making the learning curve smaller," said Lori Morrissey, Story County emergency management coordinator. Another aspect the training exercise tested was officials' ability to inform the public of immediate dangers through press conferences, Morrissey said.
Source: http://www.iowastatedaily.com/vnews/display.v/ART/2005/04/13 /425ca49db2963

21. *April 13, RCR Wireless News* — **DHS official calls for cellular carriers to move off 800 MHz.** An official in the Department of Homeland Security said Tuesday, April 12, that the cellular−phone industry should give up some of its spectrum in the 800 MHz band to help first responders have less congested airways. J. Richard Berman, DHS assistant inspector general for audits, appeared before the House Homeland Security emergency preparedness subcommittee as the panel examined a bill to streamline and provide greater oversight to first−responder grants. Berman said one of the major problems facing first responders across the nation was interoperable communications, and that long term, the way to solve this problem was for the Federal Communications Commission to allocate more spectrum for public−safety communications. Even if first responders get the right equipment to operate in the 800 MHz band, it becomes "overwhelmed" in a crisis, said Berman, noting that "it will take a long time to migrate the cell−phone companies off of the 800 MHz band." "Ultimately first responders need both the same equipment or the codes to know what others are using and more spectrum," he

said.
Source: http://rcrnews.com/news.cms?newsId=22199

[Return to top]

Information Technology and Telecommunications Sector

22. *April 14, Agence France Presse* — **Japan suspects cyber attack on official Websites.** Japan's police and defense agencies said they had come under cyber attack, amid reports a Chinese website was calling for the jamming of Japanese servers amid a heated bilateral disagreement. "Access to the homepage of the National Police Agency was hampered from around 9:00 pm (1200 GMT Wednesday, April 13) to 3:00 am (1700 GMT)," the national police said in a statement. "We are investigating the cause but it is highly possible that it was a cyber attack in which a large volume of information was sent to the address of the homepage," it said. Japanese media reports said a Chinese website had urged Internet users to flood Japanese servers with irrelevant data. A police spokesperson said the agency was "aware of the call" from China but had not identified what hampered the access. The Defense Agency also said its Website had been experiencing access problems from late Wednesday, April 13. Tensions have been rising between Japan and China. Japan announced Wednesday that its companies would have the right to drill for oil and gas in an area of the East China Sea bitterly disputed between the Asian economic powers.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1509&ncid=738&e=11&u=/afp/20050414/tc_afp/japanchinainternet

23. *April 14, Thanh Nien News (Vietnam)* — **Vietnamese government Websites attacked.** In recent days, several Vietnamese Websites including some government sites have been defaced and a Turkish hacker is claiming responsibility for the attacks. The hacker calls himself iSKORPiTX. After the attacks, he posted a list of hacked Websites on the Internet at http://www.zone−h.org. He said that five Vietnamese Websites were hacked into in just one day on April 11, including some government Websites with the domain names gov.vn and edu.vn. Hacker iSKORPiTX has claimed to deface 316 Websites. Currently, the hacker ranks fourth on the top 10 list of world Website hackers. He said that he randomly liked to hack into Websites, but had no dark intentions.
Related article on hacked Anchorage airport Website:
http://www.usatoday.com/travel/news/2005−04−13−ala−airport−h acking_x.htm
Source: http://www.thanhniennews.com/society/?catid=3&newsid=6150

24. *April 14, CNET News* — **Worm attack forces Reuters instant messaging offline.** Reuters has shut down its instant messaging (IM) system after suffering an onslaught from a new Kelvir worm, the company confirmed Thursday, April 14. The London−based international media company decided to take its Reuters Messaging system completely offline after noticing the attack on its network earlier on Thursday. The new variant attempted to spread by sending fake instant messages to people in contact lists on infected systems. The messages, crafted to look exactly like legitimate IM correspondence, attempted to lure people to a Website where their computers would be infected with Kelvir. Unlike the free IM software marketed by America Online, Microsoft and Yahoo, Reuters Messaging was created as a corporate tool, closed off from public subscribers and for internal company use only. But in recent years, the company

has moved to connect its consumers with those networks. Technical workers at Reuters said they believe the new Kelvir attack could also target other IM systems. No other companies with messaging software had reported such a threat as of midday Thursday, however.
Source: http://news.com.com/Worm+attack+forces+Reuters+IM+offline/2100-7355_3-5671139.html?tag=nefd.top

25. *April 14, Government Accountability Office* — **GAO-05-550T: Market Developments in the Global Satellite Services Industry and the Implementation of the ORBIT Act (Testimony).** In 2000, the Congress passed the Open-market Reorganization for the Betterment of International Telecommunications Act (ORBIT Act) to help promote a more competitive global satellite services market. The ORBIT Act called for the full privatization of INTELSAT, a former intergovernmental organization that provided international satellite services. Most of the stakeholders the Government Accountability Office (GAO) spoke with said that access to non-U.S. satellite markets has generally improved during the past decade. This improvement in market access is generally attributed to global trade agreements and privatization trends. Despite this general view, some satellite companies expressed concerns that some market access issues still exist. For example, some companies noted that some countries may favor domestic satellite providers or may choose to continue obtaining service from Intelsat because of long-term business relationships that were forged over time. Nevertheless, Intelsat officials noted that it seeks market access on a transparent and nondiscriminatory basis and that Intelsat has participated with other satellite operators, through various trade organizations, to lobby governments to open their markets.
Highlights: http://www.gao.gov/highlights/d05550thigh.pdf
Source: http://www.gao.gov/cgi-bin/getrpt?GAO-05-550T

26. *April 13, Reuters* — **Florida wins injunction against spammers.** The state of Florida won its first victory against spam e-mail when a judge granted an injunction against two men accused of running mass e-mailing operations, the state prosecutor said Tuesday, April 12. Florida Attorney General Charlie Crist said the injunction preventing the men from sending any more deceptive e-mails was part of his department's first prosecution under an antispam law passed by the state legislature last year. The e-mails took recipients to Websites that Crist said were engaged in fraudulent or illegal activities, such as selling pharmaceuticals and cigarettes online or providing a platform for the illegal downloading of copyrighted movies. A national antispam law took effect at the start of 2004 but has done little to curb the flood of spam clogging e-mail in-boxes. Spam is estimated to account for more than 80% of all e-mail traffic, costing businesses billions a year in lost productivity and bandwidth.
Source: http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,101051,00.html?source=NLT_PM&nid=101051

27. *April 13, CNET News* — **Second broadband outage in a week strikes Comcast.** Comcast's high-speed Internet service on Tuesday, April 12, suffered nationwide outages for the second time in six days, which the cable giant blamed on issues related to its domain name servers. The three-hour outage came after a similar issue hit Comcast on Thursday, April 7, for six hours. Both involved issues with the cable giant's domain name servers, which translate and route Web page requests from users. Although Internet applications such as instant messaging could continue to operate, Website requests either did not respond or were sluggish. "We were able to identify the situation right away," Comcast spokesperson Jeanne Russo said. "We are working

with the (hardware) vendor to make sure it doesn't happen again." Comcast is the nation's largest broadband Internet access provider. It reported seven million subscribers at the end of 2004.
Source: http://news.com.com/Another+broadband+outage+strikes+Comcast/2100−1034_3−5669961.html?tag=nefd.top

28. *April 13, Techworld* — **IP flaw could allow attacks on routers and Internet software.** The UK's National Infrastructure Co−Ordination Center (NISCC) has warned of a flaw in Internet Protocol (IP) that could allow significant attacks on a wide range of products, including routers and Internet software from Microsoft, Cisco Systems, IBM, Juniper Networks, and others. While the flaw in ICMP, IP's control protocol, will be only moderately critical for some vendors' products, in others it could allow a denial−of−service attack with medium−term effects, effectively putting the system out of commission for a significant period of time while it is reset, the NISCC said in an advisory. In other products, attacks could merely slow down traffic or result in short−term denial−of−service. "Most vendors include support for this protocol in their products and may be impacted to varying degrees," the agency said in its advisory.
NISCC Advisory: http://www.niscc.gov.uk/niscc/docs/al−20050412−00308.html?la ng=en
Source: http://www.infoworld.com/article/05/04/13/HNipflaw_1.html?SE CURITY

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: Microsoft has released a Security Bulletin Summary for April 2005. This summary includes several bulletins that address vulnerabilities in various Windows applications and components. Exploitation of some vulnerabilities can result in the remote execution of arbitrary code by a remote attacker.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 20525 (−−−), 1026 (−−−), 139 (netbios−ssn), 41170 (−−−), 4672 (eMule), 1027 (icq), 53 (domain), 6346 (gnutella−svc) 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

29. *April 14, AFX* — **Counterfeit industries going global, link up with crime rings.** Counterfeit industries are becoming increasingly global, linking up with international crime rings and terrorists, a French intellectual property rights official said. Benoit Battistelli, head of the French National Institute for Industrial Property, said that to fight piracy now requires international coordination and cooperation on an unprecedented scale. “It's expanding and becoming more and more industrialized. It does not only involve little producers trying to copy some brand name products but networks which are organized internationally,” he said. These networks have links with organized international crime rings and in some cases are connected with terrorists, he said. “It requires well−coordinated efforts for all the countries concerned to uncover, trace and destroy organized international crime rings,” Battistelli said. Battistelli said other countries should pass new laws, as France has done, to punish not only producers and distributors but consumers of counterfeit goods as well.
Source: http://uk.biz.yahoo.com/050414/323/fgbl8.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 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