Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 14 April 2005

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

Daily Highlights

- TheBostonChannel reports that thousands of Tufts University alumni have been left vulnerable to identity theft after a computer security breach. (See item 6)
- The Anchorage Daily News reports Sunday's attack on the Anchorage International Airport's Website underscored a broader computer security issue state officials have been grappling with for months. (See item 11)
- Reuters reports scientists are rushing to destroy a flu virus that was sent to laboratories around the world as part of routine test kits, but which could trigger a pandemic should it escape. (See item 18)

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 13, Associated Press* — **Statoil shuts down oil drilling rig.** Oil exploration drilling from the offshore rig Eirik Raude has been shut down after its third spill into ecologically fragile Arctic waters in just over two months, Statoil ASA announced Wednesday, April 13. The Norwegian parliament has allowed oil companies to search for petroleum in the Barents Sea off northern Norway on the condition that there are no emissions into the Arctic waters. The

state−controlled Statoil said the rig spilled about 1.75 tons of hydraulic oil into the water on Tuesday, April 12, probably from a hydraulic hose. Tim Dodson, Statoil's senior vice president for exploration on the Norwegian continental shelf, said drilling would not resume until they were certain that there would be no future spills. Drilling began on April 2. The Barents Sea north of Norway and Russia is believed to have vast oil and natural gas reserves, crucial for Norway to maintain levels of oil production that make the Nordic nation the world's third largest oil exporter after Saudi Arabia and Russia.
Source: http://www.washingtonpost.com/wp−dyn/articles/A49317−2005Apr 13.html

2. *April 13, Federal Energy Regulatory Commission* — **Commission approves new gas projects.** The Federal Energy Regulatory Commission (FERC) on Wednesday, April 13, approved several new natural gas projects, including the construction of a new marine terminal for liquefied natural gas (LNG) and expansion of a previously approved LNG project that will increase and enhance the energy infrastructure in the Gulf Coast region of the United States. FERC approved a proposal by Corpus Christi LNG, L.P. and Cheniere Corpus Christi Pipeline Company to construct and operate a new LNG terminal and related pipeline facilities near Corpus Christi, TX. FERC also approved an amended proposal by Cameron LNG, LLC to expand its facilities in Hackberry, LA to receive larger LNG tankers at its terminal that is currently under construction. In separate decisions, FERC approved three new storage facilities. FERC Chairman Pat Wood, III said, “These facilities add much needed infrastructure to meet our Nation’s ever−increasing demand for reliable and affordable energy.”
Source: http://www.ferc.gov/press−room/pr−current/04−13−05−gas.asp

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *April 13, Seattle Post−Intelligencer* — **Tanker truck spill blocks major interstate.** Motorists were brought to a halt Tuesday morning, April 12, when a truck pulling a tanker of hot roofing tar lost its trailer, which rolled and spilled enough tar to cover all lanes of northbound Interstate 5 in downtown Seattle, WA. Seattle firefighters used hoses to cool the tar, which was scraped up with a front−end loader once it hardened. Troopers are investigating how the trailer became dislodged. There were no injuries, and all lanes were reopened to traffic about 2:15 p.m. The driver of the vehicle was cited for "speed too fast for conditions."
Source: http://seattlepi.nwsource.com/local/219951_tarspill13.html

[Return to top]

Defense Industrial Base Sector

4. *April 13, Government Accountability Office* — **GAO−05−520T: DoD High−Risk Areas: Successful Business Transformation Requires Sound Strategic Planning and Sustained Leadership (Testimony).** In January 2005, Government Accountability Office (GAO) released its 2005 high−risk series update report for the 109th Congress. GAO’s high−risk series has increasingly focused on major government programs and operations that need urgent attention and transformation to ensure that the U.S. government functions in the most economical,

efficient, and effective manner possible. GAO also emphasizes those federal programs and operations that are at high risk because of their greater vulnerabilities to fraud, waste, abuse, and mismanagement. Of the 25 areas on GAO's 2005 high−risk list, eight are Department of Defense (DoD) programs or operations and six are government−wide high−risk areas for which DoD shares some responsibility. DoD's failure to effectively address these many high−risk areas results in billions of dollars of waste each year and inadequate accountability to Congress and the American people. The Subcommittee asked GAO to provide its views on (1) DoD's high−risk areas, including those it shares responsibility for with other federal agencies; (2) an emerging challenge for DoD that merits close attention, involving DoD's approach to risk management; and (3) key elements, such as a chief management official, to successfully address these high−risk areas and achieve business transformation reform.
Highlights: http://www.gao.gov/highlights/d05520thigh.pdf
Source: http://www.gao.gov/new.items/d05520t.pdf

[Return to top]

Banking and Finance Sector

5. *April 13, Image and Data Manager (Australia)* — **New phishing attacks based around authentication.** A white paper has been released about the dangers of first−generation authentication, because it presents an opportunity for fraud and phishing attacks. The white paper, called "Vulnerability of First−Generation Digital Certificate and Potential for Phishing Attacks and Consumer Fraud," claims that organization−validated certificates are not only prone to human error but it is easy for a disreputable person or entity to request a certificate in a well−known company name, and then create a phishing site to defraud customers. This could especially be a large risk when it is viewed in a browser that displays the organization name with the secure sockets layer, which indicates that the Website is legitimate. Howard A. Schmidt, former White House cyber security advisor, said, "Manual vetting of organizations creates a huge vulnerability that can be used to the benefit of phishers and identity thieves. I hope that certification authorities who are still using first−generation processes will understand why they should migrate to advanced authentication without delay." The white paper was written by Kirk Hall of GeoTrust, a provider of Web security services.
White Paper: http://www.geotrust.com/resources/white_papers/pdfs/SSLVulnerabilityWPcds.pdf
Source: http://www.idm.net.au/story.asp?id=6272

6. *April 12, TheBostonChannel.com (MA)* — **Tufts alumni warned of computer−system theft.** Thousands of Tufts University alumni have been left vulnerable to identity theft after a computer security breach. The university sent a letter to more than 100,000 alums saying, "There's no indication that any information had been retrieved or was being misused." According to the university's letter, "the intent of the intruder may have been to use the computer as a distribution point for movies and other entertainment media files." However, the officials at the university, located in Medford, MA, suggested alums take steps to ensure their private information was not misused.
Source: http://www.thebostonchannel.com/newsarchive/4371082/detail.h tml

7.

April 12, BusinessWeek — **A hacker break−in affects Northwestern University.** The Kellogg School of Management at Northwestern University in Evanston, IL, is investigating a recent security breach on its computer network. On March 20, while most students were away on spring break, Northwestern University's information technology (IT) department noticed that two Kellogg servers were sending anomalous traffic onto the university network. The IT group blocked this traffic from the broader network and alerted Kellogg. Investigations uncovered hacking activity on multiple computers and also revealed that the hacker had most likely gathered user ID and password information from the Kellogg domain. No reports have yet surfaced of unauthorized use of personal information as a result of the security breach, said David Keown, Kellogg's chief information officer and assistant dean for information technology.
Source: http://www.businessweek.com/bschools/content/apr2005/bs20050412_1226_bs001.htm

[Return to top]

Transportation Sector

8. *April 13, Government Accountability Office* — **GAO−05−333SP: National Airspace System: Experts' Views on Improving the U.S. Air Traffic Control Modernization Program (Report).** In 1981, the Federal Aviation Administration (FAA) began a program to modernize the national airspace system and a primary component, the air traffic control (ATC) system. The ATC component of this program, which is designed to replace aging equipment and accommodate predicted growth in air traffic, has had difficulty for more than two decades in meeting cost, schedule, and performance targets. The performance−based Air Traffic Organization (ATO) was created in February 2004 to improve the management of the modernization effort. On October 7, 2004, the Government Accountability Office (GAO) hosted a panel to discuss attempts to address the ATC modernization program's persistent problems. Participants discussed the factors that they believed have affected FAA's ability to acquire new ATC systems. Participants also identified steps that FAA's ATO could take in the short term to address these factors, as well as longer term steps that could be taken to improve the modernization program's chances of success and help the ATO achieve its mission. The participants included domestic and foreign aviation experts from industry, government, private think tanks, and academia. They are recognized for their expertise in aviation safety, economics, and engineering; transportation research and policy; and government and private sector management.
Highlights: http://www.gao.gov/highlights/d05333sphigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−333SP

9. *April 13, Agence France−Presse* — **Qantas announces security cameras for baggage handling areas.** Australian airline Qantas said Wednesday, April 13, it would install security cameras at baggage handling areas after a worker was seen frolicking around Sydney airport in a camel costume taken from a passenger's bag. The airline will place "CCTV surveillance equipment in baggage handling areas at terminals throughout Australia that are either owned or solely leased by Qantas," airline officials said in a statement. Cameras will also be installed in the holds of aircraft and at other locations in airports in addition to the 990 already in place. "We have also instigated discussions on Qantas' upgraded baggage security requirements with

the owners and operators of other terminals in Australia and overseas where Qantas operates," said chief executive officer Geoff Dixon. Dixon said the decision to upgrade security was taken because of increased public concern about the safety of their baggage. Passenger David Cox last week complained when he saw a Qantas staffer wearing his camel's head on the tarmac 20 minutes after he had checked it in as part of his luggage. The costume was returned to its owner and the baggage handler dismissed but the case has raised concerns about luggage security.
Source: http://www.usatoday.com/travel/news/2005−04−13−qantas−camera_s_x.htm

10. *April 13, WJZ 13 (MD)* — **Tunnel safety recommendations implemented.** Baltimore and CSX officials say they've put in place the railroad safety recommendations demanded by federal transportation officials. The National Transportation Safety Board (NTSB made the recommendations after concluding its investigation into the 2001 train derailment and fire in the Howard Street tunnel. The city reported that it is communicating better with CSX and is more prepared for an emergency situation in a tunnel. In a letter to the NTSB, Baltimore Fire Chief William Goodwin said the department has more equipment to help crews breathe in a tunnel fire environment and more people trained to use it than four years ago. A CSX freight train partially derailed in the Howard Street Tunnel on July 18, 2001. Four of the 11 cars that derailed were tankers carrying flammable and hazardous chemicals. One of them ruptured, igniting a fire, which created an inferno in the tunnel that paralyzed the downtown area for days. Tuesday, April 12, was Baltimore's deadline to respond to the NTSB.
For NTSB documentation refer to Abstract: 7662. National Transportation Safety Board Safety Recommendation Date: January 5, 2005. http://www.ntsb.gov/recs/letters/2004/r04_15_16.pdf
and
Abstract: 7662. National Transportation Safety Board Recommendation Date: January 5, 2005
http://www.ntsb.gov/recs/letters/2004/r04_15_16.pdf
Source: http://wjz.com/localstories/local_story_103064123.html

11. *April 13, Anchorage Daily News (AK)* — **Hacker invades Alaskan airport Website.** Travelers logging on to check flight information on Ted Stevens Anchorage International Airport's Website Sunday, April 10, got a surprise. Instead of a list of arrival and departure times, they were greeted by a waving Turkish flag, with a steely−eyed man's face in the lower right corner. Beneath it was a message crediting a Turkish hacker who goes by the handle "iSKORPiTX" for the cybervandalism. Sunday's attack, while relatively harmless, underscored a broader computer security issue state officials have been grappling with for months. The hacker gained access only to the airport's Web server, not its internal network, on which financial documents, e−mails and other data are stored, airport director Mort Plumb said. "No other parts of any infrastructure at the airport were affected by this," Plumb said. The hacker behind Sunday's attack is fairly well known in Internet circles and doesn't try to hide his or her tracks. A hacker Website that chronicles such exploits gives iSKORPiTX credit for defacing hundreds of other Websites, including state government sites in Iowa, Georgia, and Tennessee.
Source: http://www.adn.com/news/alaska/story/6374493p−6252421c.html

12. *April 13, TheBostonChannel.com (MA)* — **Lighter ban on planes to take effect.** Baggage screeners at airports around the nation will begin enforcing a new law Thursday, April 14, that prohibits passengers from carrying a lighter past security checkpoints and packing lighters in their carry−on baggage. One mandate of the Intelligence Reform and Terrorism Prevention Act of 2004 added butane lighters to the list of items passengers are not allowed to carry on

airplanes. The Transportation Security Administration (TSA) said the ban was put in place to ensure passenger safety and security. The ban includes butane, absorbed−fuel (Zippo−type), electric/battery−powered and novelty lighters. Officials said matchbooks are being allowed past checkpoints and on planes because a match cannot hold a flame as long as a lighter and because it also releases a smell that would alert other travelers and the flight crew.
For additional information see
http://www.tsa.gov/public/display?theme=183&content=09000519 80115b30
Source: http://www.thebostonchannel.com/travelgetaways/4375291/detai l.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *April 13, Associated Press* — **State of Texas to randomly test for tuberculosis in cattle.** Instead of voluntary testing, Texas will randomly check beef herds for tuberculosis (TB) in its effort to regain the federal government's crucial TB−free designation. Texas, the nation's leading cattle producing and exporting state, lost the U.S. Department of Agriculture's (USDA) TB−free status in 2002 after two infected cattle herds were detected. Rather than restrict the state's beef exports, the USDA approved a voluntary testing program devised by industry representatives and the Texas Animal Health Commission. Under the new plan, about 2,400 beef herds −− an average size herd is about 40 animals −− are to be tested by the end of the year. As of this week, only about 515 of the 153,000 herds had been tested. Bovine TB is a highly contagious lung bacteria, spread by infected cattle coughing, bellowing, and snorting in the confines of a feedlot or pasture. Herds will be randomly selected from a commission database listing breeder cattle owners, said Dee Ellis, a veterinarian with the commission who manages the testing program.
Source: http://www.tallahassee.com/mld/tallahassee/business/11380843 .htm

14. *April 12, DTN Soybean Rust Information Network* — **Third Florida county reports rust.** Florida's third positive find of Asian soybean rust (ASR) provides even more reason to believe the fungus will continue to spread northward as spring progresses, said officials at the University of Florida's Division of Plant Industry on Tuesday, April 12. Tim Schubert, a plant pathologist at the Florida facility, said the latest ASR find in Marion County was on a kudzu leaf located north and east of the two March finds in Pasco and Hernando counties. As many U.S. South crop experts search for rust spores on kudzu plants and early−planted soybeans, Florida remains the only state with positive ASR cases in 2005. Schubert is still trying to determine just how the spores arrived in the Marion County kudzu patch. "It's unlikely the spores flew into this area from the other two counties, it just happened to land in exactly the same spot where we had pronounced disease activity last year," Schubert said. Schubert added, "I'm thinking there must have been some spore survival from last year. Even though all of the foliage was knocked off this kudzu it has emerged with new growth, and there is a little bit of

rust starting to show up now."
Source: http://www.dtnsoybeanrustcenter.com/index.cfm?show=10&mid=26 &pid=45

[Return to top]

Food Sector

15. *April 11, Food and Drug Administration* — **Tahini recalled.** Ziyad Brothers Importing is voluntarily recalling its Ziyad brand Tahini due to possible contamination with Salmonella Senftenberg. The possible contamination was noted after testing by the Minnesota Department of Agriculture and the Illinois Department of Public Health. Salmonella Senftenberg is an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. In rare circumstances, infection with Salmonella can result in the organism getting into the bloodstream and producing more severe illnesses such as arterial infections, endocarditis, and arthritis. No illnesses have been reported to date in connection with the Ziyad brand Tahini. The product is distributed nationwide.
Source: http://www.fda.gov/oc/po/firmrecalls/ziyad04_05.html

16. *April 10, New York Times* — **Stores say wild salmon, but tests say farm bred.** Fresh wild salmon from West Coast waters used to have a low profile in New York: it generally migrated eastward in cans. But a growing concern about the safety of farm−raised fish has given fresh wild salmon cachet. Today, "fresh wild salmon" is abundant, even in the winter when little of it is caught. Tests performed for The New York Times in March on salmon sold as wild by eight New York City stores, going for as much as $29 a pound, showed that the fish at six of the eight were farm raised. Farmed salmon, sells for five dollars to 12 dollars a pound. The findings mirror suspicions of many in the seafood business that wild salmon could not be so available from November to March, the off−season. Wild and farmed salmon fillets and steaks look similar because farmed fish are fed artificial coloring that makes them pink, but that coloring can be measured in laboratory testing. With East Coast wild salmon all but extinct and West Coast wild catches restricted by quotas, farmed fish constitute 90 percent of U.S. salmon sales. Yet last month, when fresh wild salmon should have been scarce, 23 of 25 stores checked by The Times said they had it in stock.
Source: http://www.nytimes.com/2005/04/10/dining/10salmon.html?oref= login

[Return to top]

Water Sector

17. *April 11, American Water Works Association* — **Water and security officials explore monitoring technologies.** Officials charged with protecting North American water supplies examined the latest contamination warning technologies Monday, April 11, during the third annual Water Security Congress, hosted by the American Water Works Association (AWWA). More than 350 water professionals, security officials and emergency responders participated in the Oklahoma City gathering, which took place one week before the 10th anniversary of the Alfred P. Murrah Federal Building terrorist bombing. During the congress, AWWA released a

new report, "Contamination Warning Systems for Water: An Approach for Providing Actionable Information to Decision−Makers," that summarizes the state of science on contamination monitoring technologies and explores how utilities can manage complex data collected. In addition, more than 50 manufacturers of cutting−edge monitoring devices and other security technologies displayed their products for utility officials. AWWA estimates that U.S. water utilities have spent more than $2 billion since September 11, 2001, to upgrade the physical security of treatment plants and infrastructure. Utilities are also upgrading defenses against cyber−attacks on water systems and revisiting emergency response plans.
Report: http://www.awwa.org/Advocacy/contamination_warning_systems.p df
Source: http://www.awwa.org/Advocacy/pressroom/pr/

[Return to top]

Public Health Sector

18. *April 13, Reuters* — **Scientists rush to destroy flu virus.** A killer flu virus, sent to laboratories around the world as part of routine test kits, could trigger a pandemic if it escapes, but the chances of that are low, the World Health Organization (WHO) said on Wednesday, April 12. Senior WHO scientist Klaus Stohr said the virus, which killed between one million and four million people in 1957, had been sent to about 3,700 laboratories, nearly all in the U.S. The U.S. concern that sent out the virus, the College of American Pathologists (CAP), has issued instructions for all samples to be destroyed and would report to the WHO and U.S. health authorities by Friday, April 15, on the response, Stohr said. The 1957 virus has not been used in anti−flu vaccines since 1968, meaning anyone born after that date would carry no immunity to the bug. It went to some 61 laboratories outside North America, all of which had been contacted, Stohr said. But it was not certain that all U.S. recipients had been located yet, Stohr said. He noted that the first batches had been delivered as long ago as last October and that so far there were no reports of any infection.
World Health Organization: http://www.who.int/csr/disease/influenza/h2n2_2005_04_12/en/
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=topNew s&storyID=2005−04−13T093909Z_01_ZWE332233_RTRUKOC_0_HEALTH−F LU.xml

19. *April 13, Associated Press* — **Angola fights to contain outbreak.** Disease experts struggling to contain the largest recorded outbreak of the Marburg virus said Tuesday, April 12, it will take weeks to determine whether a long−term crisis can be averted in Angola, where the disease already has killed at least 194 people. The experts say they are recruiting tribal elders and musicians to help educate villagers who are hiding infected family members and have attacked aid groups sent to check the virus' spread in the southwest African nation. The World Health Organization (WHO), which already has 50 experts in the field helping local authorities, is bolstering its team by flying in more specialists. The medical aid group Doctors Without Borders also has a heavy presence on the ground, and the U.S. Centers for Disease Control and Prevention has sent experts to Uige province in northern Angola. The Angola outbreak involves 214 known cases so far. The focus is on detecting infections early, isolating those infected, training local hospitals on infection control, and removing dead bodies, which can spread the disease, said WHO spokesperson Maria Cheng. Scientists at the U.S. Army Medical Research Institute of Infectious Diseases are investigating whether a drug that has shown promise against Ebola might work against Marburg.

Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/world/ 11377546.htm

20. *April 13, Associated Press* — **Wisconsin man diagnosed with measles.** Health officials are screening people who came into contact with a man who contracted measles, the first case of the disease in Wisconsin since 1996. The state Department of Health and Family Services said Tuesday, April 12, lab tests have confirmed the man has measles, which he likely contracted on a recent trip to Germany. State health officer Herb Bostrom said the disease has been eliminated from Wisconsin, and the few cases contracted since 1996 were in travelers. Bostrom said measles is a serious illness, and outbreaks at Wisconsin day care centers as recently as the 1980s caused several deaths. Measles is easily and quickly transmitted in the air through coughing or sneezing and can affect anyone who has not previously had the disease or been vaccinated against it.
Measles Fact Sheet: http://dhfs.wisconsin.gov/communicable/communicable/factsheets/Measles.HTM
Source: http://seattlepi.nwsource.com/national/apscience_story.asp?category=1500&slug=Measles

21. *April 13, Associated Press* — **Bird flu widespread in Mekong Delta.** More than 70 percent of random duck and geese samples have tested positive for bird flu in Vietnam's southern Mekong Delta, but many farmers have refused to slaughter their flocks, officials said Wednesday, April 13. "We still don't know how strong the virus is," said Nguyen Ba Thanh, director of the Can Tho regional animal health center. "It may kill or may not kill the poultry, but it shows that the virus is entrenched in the region." Of more than 10,000 duck and geese samples gathered from poultry farms across 10 Mekong Delta provinces, 71 percent have tested positive so far this year, Thanh said. The virus also was found in about 21 percent of sampled chickens, he said. The test results suggest that more than 10 million out of nearly 20 million total birds should be slaughtered to try to stamp out the virus, he said. However, farmers are resisting local government orders to kill their flocks because of lost income.
Source: http://abcnews.go.com/Health/wireStory?id=665180

[Return to top]

Government Sector

22. *March 16, Government Accountability Office* — **GAO−05−139: Department of Homeland Security: A Comprehensive and Sustained Approach Needed to Achieve Management Integration (Report).** The creation of the Department of Homeland Security (DHS) represents one of the largest reorganizations of government agencies and operations in recent history. Significant management challenges exist for DHS as it merges the multiple management systems and processes from its 22 originating agencies in functional areas such as human capital and information technology. The Government Accountability Office (GAO) was asked to identify opportunities for DHS to improve its management integration. GAO recommends that the Secretary of DHS: (1) develop an overarching management integration strategy, and (2) provide its Business Transformation Office (BTO) with the authority and responsibility to serve as a dedicated integration team and help develop and implement the strategy. GAO also suggests that Congress monitor (1) the progress of DHS's management integration, for example, by requiring the department to periodically report the status of its efforts; and (2)

whether senior leadership has the authority to elevate, integrate, and institutionalize its management integration and reassess whether to create a new Chief Operating Officer (COO) or Chief Management Officer (CMO) position to more effectively drive this integration. DHS generally agreed with the report's recommendations.
Highlights: http://www.gao.gov/highlights/d05139high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−139

[Return to top]

Emergency Services Sector

23. *April 13, The Randolph Reporter (NJ)* — **Mock case of the plague to be released.** A May disaster drill will focus on a terrorist release of the plague at a shopping mall and emergency officials hope the lessons they learn will never be put to the real test. The premise of the mock attack, planned for Saturday, May 21, will be the release of pneumonic plague in a shopping mall, and the need to quickly vaccinate or medicate the general populace. Making the whole system work will be the town's 12−member community emergency response team (CERT) and the medical response team (MRC). Police Lt. Michael Pisano, the emergency management coordinator, said the CERT is comprised of community members with a wide variety of administrative skills. He said a benefit of being part of the program is that the volunteer and family members would be among the first to receive medications and to be protected in event of a real attack, said Pisano. One of the goals of the program is to have citizens practice going through the process without panicking. From 200 to 300 volunteers are being sought. Even with that many volunteers, some will probably be asked to go through the process more than once during the four−hour process.
Source: http://www.zwire.com/site/news.cfm?newsid=14337534&BRD=1918&PAG=461&dept_id=506888&rfi=6

24. *April 13, The Messenger (IA)* — **Simulation helps community officials prepare for emergency situations.** Webster County Emergency Management in Iowa joined city and county law enforcement agencies, school officials and hospital personnel Tuesday, April 12, in an emergency drill that started with an imaginary explosion in Newton, moved on to "rail sabotage" in Ames and ended in Fort Dodge with a "high−speed chase and standoff." Overall, the simulation left dozens dead, many others wounded and a school full of children traumatized. The drill was a training exercise for Iowa Homeland Security Region 1. It was designed to help officials know the agency's role when an emergency happens. Though none of the events of the fast−paced morning actually happened, officials sat through them in real time and got information as it became available. Fort Dodge Assistant Police Chief Doug Utley, who participated in the drill, said the drill helped him think outside the city and county boundaries in his response to the situation.
Source: http://www.messengernews.net/top_stories_full.asp?3006

[Return to top]

Information Technology and Telecommunications Sector

25. *April 13, eWeek* — **Minneapolis plans wireless network.** Minneapolis, MN plans to provide wireless Internet access to the city's business, residents, governmental officials and visitors. The city's RFP, issued Wednesday, April 13, is expected to call for a privately owned, $15 million to $20 million citywide wireless and fiber−optic network. Contracts are expected to be issued later this year. The service should be available to residents late in 2006. The network will facilitate government communications, linking city buildings, police and inspectors to the city's databases. Excess capacity will be made available to provide service to businesses, residents and guests. Rates are expected to range between $18 and $24 per month for connections of 1M bps to 3M bps.
RFP information: http://www.ci.minneapolis.mn.us/procurement/wirelessrfp.asp
Source: http://www.eweek.com/article2/0,1759,1785426,00.asp

26. *April 13, TelecomWeb* — **U.S. panel approves sale of undersea communications cable.** The Committee on Foreign Investment, a U.S. panel made up of representatives from the Treasury, Defense, Justice, Commerce, State and Homeland Security departments, approved the sale of Tyco International's undersea cable network to Videsh Sanchar Nigam (VSNL), India's largest phone and broadband company. The $130 million acquisition, announced in November 2004, had been challenged by a trio of U.S. senators as being potentially damaging to national security. VSNL is buying 60,000 kilometers of undersea communications cable spanning three continents. Most significant, the Tyco cables represent an estimated 85 percent of the world's total trans−Pacific capacity. VSNL, which is 25−percent−owned by the Indian government, had to sign a 32−page agreement to guarantee the U.S. government can continue to install court−authorized wiretaps on the network, conduct background checks on VSNL employees in the United States, take steps to prevent illegal eavesdropping on U.S. customers, and guarantee that foreign governments can't access classified or sensitive U.S. government information carried over the undersea network.
Source: http://www.telecomweb.com/news/1113416555.htm

27. *April 12, Secunia* — **KDE kdelibs PCX image buffer overflow vulnerability.** A vulnerability in KDE kdelibs, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an error in the kimgio component when processing PCX image files. This may be exploited via a specially crafted image file to execute arbitrary code via an application linked against the vulnerable library. No vendor solution available.
Source: http://secunia.com/advisories/14908/

28. *April 12, Reuters* — **High−flying robot plane could link phone networks.** Wisconsin communications company Sanswire on Tuesday, April 12, unveiled its almost−finished prototype of a hard−framed, unmanned airship – the Stratellite – designed to fly in the stratosphere 13 miles above the earth and send broadband and mobile phone signals to an area the size of Texas. Flying above the jet stream but lower than a satellite – and one−tenth the cost at $25 million to $30 million – the Stratellite also would render land−based cell−phone towers obsolete, its makers say. But that altitude is largely unused and untested, and Sanswire officer Tim Huff acknowledged the company doesn't yet have Federal Aviation Administration approval to launch an unmanned airship.
Company information on Stratellite: http://www.sanswire.com/stratellites.htm
Source: http://www.reuters.com/newsArticle.jhtml?type=technologyNews &storyID=8162328

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 (−−−), 53 (domain), 1026 (−−−), 139 (netbios−ssn), 80 (www), 1027 (icq), 113 (auth), 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 13, Sun Newspaper Online (UK)* — **Prime Minister's jet flight scare.** New Zealand's prime minister on Wednesday, April 13, escaped death after a door on her plane blew open mid−flight and the pilot was forced to make an emergency landing. Politician Helen Clark, 55, was left badly bruised after her six−seater jet plunged into a sharp descent before touching down. The door had become dislodged when the aircraft hit severe turbulence at 8,000 feet. Two security officers grabbed held it in place for more than 15 minutes while the pilot guided the plane to safety at an airport. The twin−engine plane had been en route to the capital, Wellington, from the tourism town of Rotorua in central North Island. Airline officials said an initial probe indicated that a split rubber seal had worked its way under the door's locking mechanism and popped it open.
Source: http://www.thesun.co.uk/article/0,,2−2005170583,00.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