Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 21 April 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Virginian−Pilot reports the U.S. Navy is investigating how a man managed to get on board the aircraft carrier Harry S. Truman without authorization while the Norfolk, VA−based ship was visiting Britain. (See item 5)

- KOLD TV reports that after a 911 cellular phone call made by one member of an illegal alien group in distress, the Tucson Sector Border Patrol Search Trauma and Rescue Team responded, rescuing a total of 77 individuals. (See item 13)

- The Bucks County Courier Times reports an FBI agent says that Philadelphia and its suburbs foster more homegrown hate groups −− from white supremacists to radical animal rights and environmentalists −− then other U.S. areas. (See item 32)

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 20, Associated Press* — **Oil dry−up fears a myth according to OPEC official.** Global oil reserves are in little danger of running out for many decades, and the Organization of the Petroleum Exporting Countries (OPEC) will continue to boost production as necessary to stabilize prices, a senior official of the group said Wednesday, April 20. "The problem in 2004 was we did not anticipate the strength of demand ... it appears that in 2005 we are reaching a

plateau," said Adnan Shihab−Eldin, acting secretary−general of OPEC. Unusually high prices cannot continue forever, "as long as you continue to put greater supply in the market," he said. At a March meeting in Iran, OPEC increased its production ceiling by 500,000 to 27.5 million barrels a day, and provided for an identical increase if crude prices did not stabilize.
Source: http://biz.yahoo.com/ap/050420/greece_opec.html?.v=1

2. *April 20, New York Independent System Operator* — **Power agency releases trend report.** The New York Independent System Operator (NYISO) on Wednesday, April 20, released its annual state−of the−grid report, which highlights five years of improvements to the system while striking a note of caution about potential downstate supply deficiencies in the near future. Power Trends 2005 confirms that since the creation of the NYISO in 1999, significant steps have been taken to identify and resolve important industry issues. These range from planning for adequate electric generation, encouraging demand side management, breaking down barriers to the regional trade of electricity and developing renewable resources. Peak demand growth in New York continues to be modest, with the summer peak demand estimated to be 31,960 MW, up from 31,400 MW (weather adjusted) in the summer of 2004. Due to increased installed generating capacity and new regional links, such as the Cross Sound Cable (330 MW), supply is expected to exceed forecasted demand. However, supply−side deficiencies downstate are expected to impact capacity as early as 2008 if new generation projects are not commenced immediately.
Power Trends 2005 report: http://www.nyiso.com/topics/articles/news_releases/2005/ptrends2005.pdf
Source: http://www.nyiso.com/topics/articles/news_releases/2005/pr_p owertrends_042005.pdf

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *April 20, Wichita Eagle (KS)* — **Workers taken to hospital after chemical spill at plant.** Six employees of Wescon Products Co. in southwest Wichita, KS, suffered lung irritation after an accidental chemical spill in the plant Tuesday, April 19. Manager Steve Randall said the employees were sent to the hospital for a precautionary checkup and were given the rest of the day off after an accident caused a small release of formaldehyde gas.
Source: http://www.kansas.com/mld/kansas/news/11436995.htm

4. *April 20, Associated Press* — **Indiana plant may have released toxic chemical.** Daramic Inc., an industrial plant located about 20 miles west of Louisville, KY, might have illegally released a toxic chemical associated with nervous−system damage and cancer, the Environmental Protection Agency (EPA) said Tuesday, April 19. The plant released tens of thousands of pounds of trichloroethylene each year between 1998 and 2003, according to the EPA. The air pollution permit for the plant calls for allowing five percent of its trichloroethylene to escape, but 40 percent to 91 percent of the chemical was emitted during those years, the EPA's Chicago bureau said in a violation document. The plant's corporate parent, Charlotte, N.C.−based Polypore International Inc., makes thin plastic membranes that allow car batteries to work and recharge. Trichloroethylene is a nonflammable, colorless liquid used mainly as a solvent to remove grease from metal parts. A Polypore International spokesperson acknowledged that the EPA has legitimate concerns for those six years. But he said the company's new management

reduced its emissions of the chemical by 60 percent between 2002 and 2004.
Source: http://www.the−dispatch.com/apps/pbcs.dll/article?AID=/20050 420/APN/504200718

[Return to top]

Defense Industrial Base Sector

5. *April 17, The Virginian−Pilot* — **Britain, U.S. investigating unauthorized aircraft carrier visitor.** The U.S. Navy is investigating how a man managed to get on board the aircraft carrier Harry S. Truman without authorization while the Norfolk, VA−based ship was visiting Britain on April 9. The Truman's security force discovered the intruder while in port at a naval base in Portsmouth, in southern England. British police removed him after he was found. "After his discovery, the ship's security conducted a search of surrounding areas and found no suspicious packages or damage," said Cmdr. Dave Werner, a spokesperson for the 2nd Fleet in Virginia. While the ship, which returned to Norfolk on Monday, April 18, had not been open for public visits, crew members were allowed to bring a limited number of guests aboard, Werner said. The man, who was identified as Abdoul Masmoud Yessoufou, was arrested again less than 24 hours later after he attempted to re−enter the naval base. Yessoufou has since been banned from entering restricted areas of the base. Both British and U.S. authorities are investigating, Werner said.
Source: http://home.hamptonroads.com/stories/story.cfm?story=85110&r an=193571

[Return to top]

Banking and Finance Sector

6. *April 20, Finextra Research* — **British bank urges online banking customers to tighten personal computer security.** British bank Lloyds TSB is urging Web banking customers to step up their IT security after research conducted by the bank indicated that over half of consumer PCs and laptops have been infected with a computer virus. The survey of 1400 people showed that three quarters of computer users were worried about the threat of viruses, but 10% had never updated their anti−virus software. The research also found that one percent had no anti−virus technology installed at all. Matthew Timms, Internet banking director, Lloyds TSB, says: "While we are doing everything we can to make our security watertight, we also urge all of our customers to think carefully about the measures they have taken to protect their PC. This means regularly updating their anti−virus software and ensuring they have a robust firewall." Cost was the main reason given for not updating anti−virus software, although some respondents claimed that they didn't know it was necessary, or didn't know what to buy.
Source: http://www.finextra.com/fullstory.asp?id=13553

[Return to top]

Transportation Sector

7. *April 20, Transportation Security Administration* — **Response to the "Follow−Up Audit of Passenger and Baggage Screening Procedures at Domestic Airports" Inspector General**

Report. Mark O. Hatfield, Jr., Assistant Administrator of Communications and Public Information Transportation Security Administration said, "We agree with the Inspector General's conclusion that significant improvements in performance will only be possible with the introduction of new technology. That said, we will continue to seek incremental gains in screener performance through training, testing and management practices."
Follow−Up Inspector General Audit Report:
http://www.tsa.gov/public/interweb/assetlibrary/Screener_IG_ Report.pdf
Source: http://www.tsa.gov/public/display?theme=46&content=090005198 011a685

8. *April 20, Transportation Security Administration* — **Response to the "Irregularities in the Development of the Transportation Security Operations Center" Inspector General Report.** Mark O. Hatfield, Jr., Assistant Administrator of Communications and Public Information Transportation Security Administration said, "The Transportation Security Operations Center (TSOC) is a sophisticated command center that acts as the primary coordination point for multiple agencies dealing with transportation security on a daily basis. The events of 9/11 demonstrated the importance of instant communication among federal, state and local agencies in a crisis. This facility meets that critical need. After discovering inappropriate actions were taken by several employees with regard to purchasing decisions, the Transportation Security Administration (TSA) initiated this review by the Inspector General. Swift and decisive action has been taken against the individuals involved and TSA has already put in place a new management structure to strengthen its acquisition program to ensure responsible stewardship of taxpayer dollars."
Inspector General Report: Irregularities in the Development of the Transportation Security Operations Center: http://www.tsa.gov/public/interweb/assetlibrary/OIG_05−18_Ma r05.pdf
Source: http://www.tsa.gov/public/display?theme=46&content=090005198 011a68c

9. *April 20, New York Times* — **US Airways and America West in merger talks.** US Airways, which is operating in bankruptcy protection, and America West, a low−fare airline, are in serious discussions about a merger, a combination that would create the nation's sixth−largest airline, supplanting Southwest Airlines. People close to the talks characterized them as well along and said that a conclusion could be reached within a few weeks. America West's chief executive, W. Douglas Parker, has been a loud proponent of the need for consolidation within the industry, while US Airways has been viewed by many analysts as ripe for a takeover once it emerges from bankruptcy. US Airways, which is based in Arlington, VA, is the seventh largest airline and America West, based in Phoenix, is the eighth largest airline. The talks come amid wide calls for consolidation as a tool to lead many airlines out of billions of dollars in losses. Many chief executives, including Parker at America West, Glenn F. Tilton at United, and Gary C. Kelly at Southwest have argued that the industry is awash in too many seats, driving down prices at a time when the airlines are struggling with high costs and stiff competition.
Source: http://www.nytimes.com/2005/04/20/business/20air.html?adxnnl =1&oref=login&adxnnlx=1113996677−VmLKc8pKODYqzuafoRcdHA

10. *April 20, Associated Press* — **Audit cites TSA waste and abuse.** A review of the Transportation Security Administration (TSA)’s crisis management center project's expenditures uncovered evidence of suspicious purchases, improper use of government purchase cards, and unethical and possibly illegal activities by federal employees, according to the report released Tuesday, April 19, by the Department of Homeland Security. The inspector

general faulted the TSA for breakdowns in management controls that "left the project vulnerable to waste and abuse." Internal reports that policies were being violated were quashed and those who cited problems were admonished to support the project manager, the report said. In a separate report, the Homeland Security inspector general said screeners were diligent and responsible but not better than they were before the September 11 attacks at detecting fake weapons and bombs undercover agents tried to smuggle aboard planes. Greater use of new technology is needed, the inspector general concluded.
Inspector General Report: Irregularities in the Development of the Transportation Security Operations Center: http://www.tsa.gov/public/interweb/assetlibrary/OIG_05−18_Ma r05.pdf
Source: http://www.11alive.com/news/usnews_article.aspx?storyid=6198 7

11. *April 20, Government Accountability Office* — **GAO−05−542T: Air Traffic Control: Preliminary Observations on Commercialized Air Navigation Service Providers (Testimony).** In the past, governments worldwide owned, operated, and regulated air navigation services, viewing air traffic control as a governmental function. But as nations faced increasing financial strains, many governments decided to shift the responsibility to an independent air navigation service provider (ANSP) that operates along commercial lines. As of March 2005, 38 nations worldwide had commercialized their air navigation services, fundamentally shifting the operational and financial responsibility for providing these services from the national government to an independent commercial authority. The Government Accountability Office (GAO) selected five ANSPs −− in Australia, Canada, Germany, New Zealand, and the United Kingdom −− to examine characteristics and experiences of commercialized air navigation services. These ANSPs used different ownership structures and varied in terms of their size, amount of air traffic handled, and complexity of their airspace. This testimony, which is based on ongoing work, addresses the following questions: (1) What are common characteristics of commercialized ANSPs? (2) What do available data show about how the safety, cost, and efficiency of air navigation services have changed since commercialization? (3) What are some initial observations that can be made about the commercialization of air navigation services?
Highlights: http://www.gao.gov/highlights/d05542thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−542T

12. *April 20, Government Accountability Office* — **GAO−05−307T: Coast Guard: Preliminary Observations on the Condition of Deepwater Legacy Assets and Acquisition Management Issues (Testimony).** In 2002, the Coast Guard began a multiyear, $19 billion to $24 billion acquisition program to replace or modernize its fleet of deepwater aircraft and cutters, so called because they are capable of operating many miles off the coast. For several years now, the Coast Guard has been warning that the existing fleet −− especially cutters −− was failing at an unsustainable rate, and it began studying options for replacing or modernizing the fleet more rapidly. Faster replacement is designed to avoid some of the costs that might be involved in keeping aging assets running for longer periods. This testimony, which is based both on current and past Government Accountability Office (GAO) work, addresses several issues related to these considerations: (1) changes in the condition of deepwater legacy assets during fiscal years 2000 through 2004; (2) actions the Coast Guard has taken to maintain and upgrade deepwater legacy assets; and (3) management challenges the Coast Guard faces in acquiring new assets, especially if a more aggressive schedule is adopted.
Highlights: http://www.gao.gov/highlights/d05307thigh.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−307T

13. *April 20, KOLD TV (AZ)* — **Border Patrol responds to distress call.** On Tuesday, April 19, a 911 cellular phone call made by one member of an illegal alien group in distress launched the Tucson Sector Border Patrol Search Trauma and Rescue Team (BORSTAR) into action, resulting in a total of 77 individuals being rescued. The Tucson Sector Communications Center received information from Emergency Services that a group of illegal aliens had called and that they were in distress. The Tucson Sector Communications Center, was able to connect the call to the BORSTAR team directly. The BORSTAR agents asked questions to narrow the search area by key landmarks. Agents input this critical information into mapping software at the Incident Command center, and were able to quickly limit the search area. They ascertained that the group was lost in the desert somewhere north of the Village of San Pedro, on the Tohono O'odham reservation, and within eyesight of the Silver Bell Mine. Approximately 15 minutes later, the caller phoned to excitedly say that they could hear the rescue helicopter. Approximately 15 minutes after the first group was located, a second group was located and rescued, several miles to the south. These people signaled the search helicopter by writing "HELP" in large letters on the sand.
Source: http://www.kold.com/Global/story.asp?S=3237324&nav=14RTYtly

14. *April 18, Government Accountability Office* — **GAO−05−558: Aviation Fees: Review of Air Carriers' Year 2000 Passenger and Property Screening Costs (Report).** The Aviation and Transportation Security Act (ATSA) authorized the Transportation Security Administration (TSA) to impose an Aviation Security Infrastructure Fee (ASIF) on air carriers to help pay for the costs of aviation security services. To impose the ASIF, TSA issued an Interim Final Rule (IFR) and required air carriers to report their passenger and property screening costs incurred in 2000 on an attachment to the IFR referred to as Appendix A. The 2000 screening costs reported by air carriers were going to be used to establish the ASIF. Based on industry estimates of $1 billion, TSA had estimated that the costs incurred by air carriers in 2000 were $750 million, but the amounts reported by air carriers totaled $319 million, significantly less than expected. To provide the Congress with an independent assessment, the Department of Homeland Security Appropriations Act of 2005 required the Government Accountability Office (GAO) to review the amount of passenger and property screening costs incurred by air carriers in 2000. GAO recommends that the Secretary of Homeland Security direct the Assistant Secretary, TSA to consider the analysis and estimates in this study in determining the limitation on the aggregate air carrier fee consistent with ATSA. TSA concurred with this recommendation. TSA indicated that it will consider the analysis and estimates in this study, as GAO recommended.
Highlights: http://www.gao.gov/highlights/d05558high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−558

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

15. *April 20, Reuters* — **Bird flu found in Italian turkeys.** Italy has detected a low−risk strain of bird flu in turkeys in one of its northern regions but the outbreak does not pose a threat to public health, the European Commission said on Wednesday, April 20. "A low pathogenic form of avian influenza was notified to the European Commission on Monday, April 18, concerning 10 turkey flocks in the province of Brescia," a Commission official told Reuters. He noted that the strain was H5N2. It was not immediately clear how many birds were affected. Italian authorities were now expected to carry out vaccinations in the area in question, the official said. Italy's Health Ministry said it would also destroy some 180,000 turkeys as a precaution. Russia's Agriculture Ministry said it had suspended imports of poultry and poultry product from Italy to prevent the spread of bird flu. The Russian ban also applies to poultry meat products subjected to thermal treatment.
Source: http://www.alertnet.org/thenews/newsdesk/L20689804.htm

16. *April 19, Iowa State University* — **Iowa State University to test Asian soybean rust fast track system.** Forrest Nutter, an Iowa State University plant pathologist, will be coordinating a test of the Iowa Soybean Rust Team's fast track system the week of April 18. "The goal of the exercise is to test the communications within the fast track system," Nutter said. "We are testing every step of the process from the grower to the diagnostic laboratory." The fast track system was set up by the Iowa Soybean Rust Team to speed up the identification of Asian soybean rust. To participate in the fast track system a grower or consultant must contact a first detector. More than 400 first detectors throughout Iowa have been trained to identify the disease. First detectors who receive suspect samples will forward them to a triage person. Forty Iowa State extension specialists have been trained as triage members to identify soybean rust. Triage members will send suspect samples to the Iowa State University Plant Disease Clinic. The first two soybean rust samples collected in Iowa are required to be sent to the U.S. Department of Agriculture National Plant Germplasm and Biotechnology Laboratory for confirmation.
Source: http://www.ag.iastate.edu/aginfo/news/2005releases/rustest.h tml

[Return to top]

Food Sector

17. *April 19, Food Safety and Inspection Service* — **Sausage products recalled.** Don Pedro's Meat, a La Puente, CA, firm, is voluntarily recalling approximately 40 pounds of sausage products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, April 19. The sausage was distributed to retail establishments in Los Angeles, CA. The problem was discovered through routine FSIS regulatory sampling. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_020_2005_Relea se/index.asp

18. *April 18, U.S. Department of Agriculture* — **Technical experts travel to Japan and Korea to facilitate resumption of U.S. beef exports.** U.S. Department of Agriculture (USDA) Secretary

Mike Johanns Monday, April 18, announced that a team of experts on Bovine Spongiform Encephalopathy (BSE) will travel to South Korea and Japan as part of the continuing efforts to resume U.S. beef and beef product exports. The delegation, led by Deputy Under Secretary for Marketing and Regulatory Programs Charles Lambert, will review how U.S. BSE prevention programs ensure the safety of U.S. beef. In addition, members of the delegation will encourage both governments to adopt import regulations that are in closer compliance with the World Organization for Animal Health (OIE) guidelines. The team will first travel to South Korea April 19−22 for technical discussions with government officials and informational sessions with local media. From April 25−27, the team will be in Japan for technical discussions and sessions with consumers, scientists, government, and business representatives. In 2003, the United States exported approximately $1.4 billion and $815 million of beef and beef products to Japan and South Korea respectively. Together these markets represented 57 percent of total U.S. exports by value.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB/.cmd/ad/.ar/sa.retrievecontent/.c/6_2_1UH/.ce/7_2_5JM/.p/5_2_4TQ/.d/1/_th/J_2_9D/_s.7_0_A/7_0_1OB?PC_7_2_5JM_contentid=2005%2F04%2F0130.xml&PC_7_2_5JM_navtype=RT&PC_7_2_5JM_parentnav=LATEST_RELEASES&PC_7_2_5JM_navid=NEWS_RELEASE#7_2_5JM

[Return to top]

Water Sector

19. *April 21, National Academies Press* — **Public Water Supply Distribution Systems: Assessing and Reducing Risks (Report).** Distribution systems of public drinking−water supplies include the pipes and other conveyances that connect treatment plants to consumer’s taps. They span almost one billion miles in the United States and include an estimated 154,000 finished water facilities. Public water supplies serve 273 million residential and commercial customers, although the vast majority of water systems serve less than 10,000 people. These distribution systems constitute a significant challenge from both an operational and public health standpoint. Furthermore, they represent the vast majority of physical infrastructure for water supplies, such that their repair and replacement represent an enormous financial liability. In 2000, the Federal Advisory Committee for the Microbial/Disinfection Byproducts Rule (M/DBPR) recommended that Environmental Protection Agency (EPA) evaluate available data and research on aspects of distribution systems that may create risks to public health. To aid in this process, EPA requested that the National Academies’ Water Science and Technology Board assemble a committee to conduct a study of water quality issues associated with public water supply systems. In this first report, the committee considered trends relevant to the deterioration of distribution−system water quality, and identified and prioritized issues of greatest concern for distribution systems.
Source: http://www.nap.edu/openbook.php?record_id=11262

20. *April 20, Muskegon Chronicle (MI)* — **Organisms in ships' ballast water threatens great lakes.** Oceangoing freighters which are supposed to be clean before entering the Great Lakes carry billions of foreign organisms into the freshwater seas each year, including saltwater algae, invertebrates and potentially deadly bacteria. According to a recent study by the University of Michigan and National Oceanic and Atmospheric Administration, freighters that enter the lakes

via the St. Lawrence Seaway routinely carry thousands of viable organisms in muddy water that sloshes around in empty ballast tanks. Those organisms can escape when ships take on and unload ballast water while in Great Lakes harbors. Ballast water is stored in huge tanks below deck to keep ships stable and is added or dumped based on the cargo load. Researchers also found that two−thirds of the 42 ships sampled carried potentially deadly organisms in ballast water tanks that were supposed to be empty and clean, including cholera and cryptosporidium. The study's authors said immediate action is needed to stem the flow of exotic organisms and pathogens entering the lakes in freighters' ballast tanks. One possible remedy: Requiring all transcontinental freighters to completely empty and refill ballast tanks with salt water before entering the Great Lakes.
Source: http://www.mlive.com/search/index.ssf?/base/news−6/111392372 7250340.xml?muchronicle?NEM

[Return to top]

Public Health Sector

21. *April 20, Reuters* — **Cambodian bird flu suspect dies in Vietnam.** A 20−year−old Cambodian woman who was rushed to a Vietnamese hospital with suspected bird flu, died Wednesday, April 20, the World Health Organization (WHO) said. The woman from Kampot province had been taken across the nearby Vietnamese border suffering a high fever and respiratory problems, symptoms of the H5N1 virus that has killed 51 people in Asia, Vietnam's Tuoi Tre newspaper said. Three Cambodians from Kampot province have already died of the bird flu virus, along with 12 Thais and 36 Vietnamese. The virus is now endemic in several areas of Southeast Asia and Vietnam, the country hit hardest, says it does not expect to be able to contain bird flu until at least 2007 because the way it is spreading still baffles experts.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=8236418

22. *April 20, Agence France Presse* — **Angola's Marburg death toll climbs but at slower rate.** Angolan health officials said that the death toll from the Marburg virus was climbing still, reaching 239, but at a slower rate as more citizens were joining in a mass effort to stamp out the disease. Out of a total 264 cases detected since October 13 in Angola, 239 people have died with the overwhelming number of fatalities in the northern Uige province where the death toll stood at 223, according to the health ministry and the World Health Organization (WHO). A total of 518 people were under observation of whom 406 were in Uige after coming in contact with the virus that can kill a person within a week. "This trend towards a reduction in cases and deaths is due to the strong mobilization of the population in the province of Uige," said health ministry spokesperson Carlos Alberto. "We can't say that we have absolute control of the Marburg disease as long as there is even one case in the country," said the representative for the WHO in Angola, Diallo Fatoumata Binta.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=15 07&e=5&u=/afp/20050420/hl_afp/angolahealthvirus_050420142457

23. *April 20, Canadian Institute for Health Information* — **Severe Acute Respiratory Syndrome outbreak resulted in fewer emergency department visits.** New data compiled by the Canadian Institute for Health Information (CIHI) show that even four months after the peak of the Severe Acute Respiratory Syndrome (SARS) outbreak in April 2003, significantly fewer

people in Ontario, Canada, used emergency department (ED) services than in the previous year. In fact, a reduction of more than five percent could still be seen in the Greater Toronto Area (GTA) eight months later. It was 10 months before ED visits to GTA hospitals returned to 2002 levels. Visits to hospital emergency departments fell not only within the GTA −− but also across the entire province. The drop in ED visits between 2002 and 2003 was most pronounced in “infected” facilities (down 45 percent during the peak of the outbreak). Hospitals in “non−infected” areas (outside the GTA) experienced a 16 percent decrease in ED visits. "These data show that the drop in emergency department visits was sustained well beyond the SARS outbreak," says Kira Leeb, Manager of Health Services Research, CIHI. "Understanding how the use of health services changed in both the short term and long term provides a new perspective on how we use emergency departments and may also help us better prepare for future outbreaks of infectious disease."
Source: http://secure.cihi.ca/cihiweb/dispPage.jsp?cw_page=media_20a pr2005_e

[Return to top]

Government Sector

24. *April 20, Government Accountability Office* — **GAO−05−573T: Homeland Security: Overview of Department of Homeland Security Management Challenges (Testimony).** The Department of Homeland Security (DHS) plays a key role in coordinating the nation’s homeland security efforts with stakeholders in the federal, state, local, and private sectors. While the Government Accountability Office (GAO) has conducted numerous reviews of specific DHS missions, such as border and transportation security and emergency preparedness, this testimony addresses overall DHS management issues. This testimony addresses (1) why GAO designated DHS’s transformation as a high−risk area; and (2) the specific management challenges facing DHS. GAO designated DHS’s transformation as a high−risk area in 2003, based on three factors. First, DHS faced enormous challenges in implementing an effective transformation process, developing partnerships, and building management capacity because it had to transform 22 agencies into one department. Second, DHS faced a broad array of operational and management challenges that it inherited from its component legacy agencies. Finally, DHS’s failure to effectively address its management challenges and program risks could have serious consequences for our national security. Overall, DHS has made some progress, but significant management challenges remain to transform DHS into a more efficient organization while maintaining and improving its effectiveness in securing the homeland. Therefore, DHS’s transformation remains a high−risk area.
Highlights: http://www.gao.gov/highlights/d05573thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−573T

[Return to top]

Emergency Services Sector

25. *April 20, First Coast News (FL)* — **Emergency response training in Orange Park.** The Food Court at the Orange Park Mall in Orange Park, FL, was the scene of the detonation of a simulated dirty bomb. Sheriff's deputies, firefighters, health workers and volunteers in Clay

County took part in a "Weapons of Mass Destruction" Training Exercise today. During the exercise, several people were exposed to low levels of radiation. More than 90 law enforcement officers, health workers and firefighters had to work together. Communication was key. Other parts of the training were to test the local agencies response time and see how prepared they are in the event of an emergency. Officials tried to make it as realistic as possible. Even the Hazmat team responded. Those exposed to the radiation were decontaminated. Hazmat members washed them down. Paramedics transported them to Orange Park Medical Center. For Clay County authorities, practice makes perfect. They feel this training will make them that much more prepared if there ever is an act of terrorism.
Source: http://www.firstcoastnews.com/news/topstories/news−article.a spx?storyid=35814

26. *April 20, Eastern Arizona Courier* — **Mock disaster called success.** The sidewalks around the Pima Elementary School in Scottsdale, AZ, looked like a Hollywood set with simulated gore and plastic guns, but the props and makeup were part of an effort to add as much reality as possible to the countywide simulated disaster Saturday morning. The exercise centered around a vehicle loaded with a mysterious white powder tearing into Graham County and blowing up near the Pima Elementary School. The terrorists exited the vehicle, then rushed into the school and took hostages to keep officers at bay. The simulation was designed to stretch the capacities of area emergency services personnel so weaknesses could be identified and eliminated. All local law enforcement and fire departments participated, along with the University of Arizona Police Department, the Department of Public Safety and the Bureau of Land Management. There was also a problem with communication between the responding entities as cell phones, and some problems getting the injured to treatment. Safford Police Chief John Griffin, who helped develop the training exercise gave firefighters an opportunity to train in their hazard materials suits and use the self−contained breathing apparatus (SCBA).
Source: http://www.eacourier.com/articles/2005/04/20/local_news/news 03.txt

27. *April 19, The Paly Voice (CA)* — **Students take part in citywide disaster drill.** Palo Alto High School (Paly) in Palo Alto, CA, participated in a 50−minute disaster drill in conjunction with the City of Palo Alto. Paly, the chosen site of the earthquake simulation, was in high action as students evacuated to safety and emergency crews set up relief bases. Other simulations were held at fire stations, Cubberley Community Center, and other locations around the city. Coincidentally, the drill took place the day after the 99th anniversary of the 1906 earthquake. The simulated earthquake, which occurred along the north end of the Hayward Fault, was a large−scale disaster with scattered incidents and injuries throughout the San Francisco Bay Area and Palo Alto, according to police officer Ron Bonfiglio. Emergency crews swept though the campus searching for victims in the buildings, while aerial reconnaissance sent by the U.S. Air Force Auxiliary assessed damage from above ground, searching for crack patterns, Red Cross volunteer Alice Mansell said. Fire fighters followed the formal procedures laid out by the city's Emergency Management Plan (http://www.pafd.org/emp/index.html). The administration is now evaluating the school's performance and will make necessary modifications to the emergency plan as necessary.
Source: http://voice.paly.net/view_story.php?id=2893

[Return to top]

Information Technology and Telecommunications Sector

28. *April 19, SecurityTracker* — **Sun Solaris may let local users hijack non−privileged port services.** A vulnerability was reported in Sun Solaris. A local user may be able to start a process that binds to a non−privileged network port to hijack future connections to the service that typically runs on that port. Only network services that run on non−privileged ports (e.g., NFS, NIS) are affected.
Updates available: sunsolve.sun.com/search/document.do?assetkey=1−26−57766−1
Source: http://www.securitytracker.com/alerts/2005/Apr/1013760.html

29. *April 19, SecurityTracker* — **CVS buffer overflows and memory leaks may let remote users execute arbitrary code or deny service.** Several vulnerabilities were reported in Concurrent Versions System (CVS). A remote user may be able to trigger a buffer overflow and execute arbitrary code on the target system or cause the CVS service to crash. Some memory allocation, memory leak, and NULL pointer errors also exist and may allow a remote user to cause denial of service conditions.
Fix available (1.11.20 stable version; 1.12.12 feature version):
https://ccvs.cvshome.org/servlets/ProjectDownloadList
Source: http://www.securitytracker.com/alerts/2005/Apr/1013759.html

30. *April 19, SecurityFocus* — **Microsoft Windows Explorer preview pane script injection vulnerability.** Microsoft Windows Explorer is prone to a script injection vulnerability. This occurs when the Windows Explorer preview pane is enabled on Windows 2000 computers. If a file with malicious attributes is selected using Explorer, script code contained in the attribute fields may be executed with the privilege level of the user that invoked Explorer. This could be exploited to gain unauthorized access to the vulnerable computer. No vendor solution is currently available.
Source: http://www.securityfocus.com/bid/13248/info/

31. *April 19, vnunet* — **Report says virus writers turning from e−mail to IM.** Email worms are falling out of favor with the hacking community, according to a report investigating malicious Internet activity. Instead malware authors are increasingly subverting vulnerable instant messenger (IM) systems and using network viruses that do not require user interaction to spread. Other threats identified include botnets and increasingly intrusive adware. The report, "Malware Evolution. January−March 2005," from security firm Kaspersky Labs notes that viruses for IM systems started to appear late last year but are only now appearing in volume. Seven out of every eight IM worms attack Microsoft's MSN Messenger service. "Improved antivirus technologies, and increased user awareness of security issues are clearly forcing virus writers and hackers to use new approaches to access users' information and systems," said Alexander Gostev, senior virus analyst at Kaspersky Labs. The study identifies 40 individual IM worms in the first quarter of the year, the majority written in one of the simplest computer languages, Visual Basic (VB). It noted that use of this language indicates the authors are relatively unsophisticated coders, since VB is not widely used by experts because it is so slow to run.
Report: http://www.viruslist.com/en/analysis?pubid=162454316
Source: http://www.vnunet.com/news/1162557

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

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

Current Port Attacks

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

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

32. *April 20, Bucks County Courier Times (PA)* — **Hate groups plentiful in Pennsylvania according to FBI.** On the 10th anniversary of the nation's worst act of domestic terrorism −− the Oklahoma City bombing −− an FBI agent said Philadelphia and its suburbs foster homegrown hate groups that receive the agency's attention. "These groups seem more plentiful in Pennsylvania," said Brian Lynch, the assistant special agent in charge of the Philadelphia region's Joint Terrorism Task Force. Bucks, Chester and Montgomery counties are among the suburban areas home to hate groups, from white supremacists to radical animal rights and environmentalists, Lynch said on Tuesday, April 19. "Belonging to these groups is not against the law, but when they espouse criminal activities, that's when we become involved," Lynch said. Besides threats from hate groups, the FBI receives threats from individuals against public buildings, utilities, roads, railroads, bridges and airports, Lynch said. "The Benjamin Franklin Bridge is one of our favorite targets," Lynch said. Philadelphia's place on the map, between New York City and Washington, DC, and its history make the city and its suburbs targets for terrorists, he said. "Does Philadelphia have something that gives us what we call 'cause for pause?' All you have to do is look out my window and see Independence Hall, the Liberty Bell," Lynch said.
Source: http://www.phillyburbs.com/pb−dyn/news/111−04202005−478516.h tml

33. *April 19, Associated Press* — **Singapore official says Jemaah Islamiyah plotting attacks.** A letter written by a member of the al Qaeda−linked Jemaah Islamiyah (JI) terror network said the group is planning an attack similar to the 2002 Bali nightclub bombings, a top Singaporean official said. Minister of Home Affairs Wong Kan Seng said Indonesian authorities obtained the letter, but he did not elaborate further. "A letter recovered in Indonesia, written by a JI member, said that 12 operatives were ready to be martyrs and that plans for a Bali−style attack were underway," Wong said in a speech Monday, April 18, to intelligence officials. Wong said the letter reflected efforts of terrorists to overcome setbacks and stay a step ahead of the law by using different forms of communication. "In order to communicate clandestinely, terrorists exploited the anonymity of prepaid phone cards and the Internet. However, when they suspected that these communications were being monitored and their activities and operatives compromised, they reverted to couriers and old fashioned letter−writing," Wong said. He also said terror groups have begun to use Caucasians and converts to Islam who do not fit stereotypical terrorist profiles.
Source: http://www.newsday.com/news/nationworld/wire/sns−ap−southeast−asia−terror%2C0%2C6794451%2Cprint.story

[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

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