Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 23 March 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

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

Daily Highlights

- Newsday reports the Pew Hispanic Center says in a new report that the nation's undocumented immigrant population surged to 10.3 million last year, despite a sluggish economy and tighter border enforcement. (See item 12)
- Federal Computer Week reports the Department of Homeland Security has launched the Commercial Equipment Direct Assistance Program to help smaller communities get commercially available cutting−edge technology to better handle terrorist threats. (See item 25)

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. *March 22, Associated Press* — **Oil prices dip but still above $57 a barrel.** Oil futures prices edged lower Tuesday, March 22, but remained above $57 a barrel despite word from Organization of Petroleum Exporting Countries (OPEC) that the group was considering raising its daily quota by a half a million barrels after a similar move last week. Light, sweet crude for May delivery fell eight cents to $57.38 per barrel in electronic trading on the New York Mercantile Exchange by afternoon in Europe. Heating oil prices rose slightly to $1.5745 a gallon. In London, Brent crude dropped one cent to $55.64 a barrel on the International Petroleum Exchange. Oil is 50 percent more expensive than a year ago, but still well below the

inflation−adjusted peak above $90 a barrel set in 1980. Prices have risen by about a third so far this year, fueled by a late cold snap across the world's largest energy consumer, the United States. They also have been underpinned by a weak dollar and rising global demand at a time when there is very little excess supply available. These factors could set the stage for a more pronounced spike in prices if there is a production outage.
Source: http://www.ledger−enquirer.com/mld/ledgerenquirer/business/1 1199423.htm

2. *March 22, Hampton Union (NH)* — **Nuclear plant in New Hampshire rated safe.** The Nuclear Regulatory Commission (NRC) has given FPL Energy Seabrook Station −− located south of Portsmouth, NH −− a positive safety assessment for 2004. The NRC released its results at a public meeting at the Emergency Operations Facility in Newington last week. "It was a very good assessment," said the nuclear plant's spokesperson Al Griffith. "Our basic concern is that Seabrook operates the plant safely for the year, no automatic plant shutdowns," said on−site NRC inspector Glenn Dentel. The NRC listed nine "findings" for the nuclear power plant, all at code green, the lowest of four color−coded safety priorities. One had to do with a piece of graph−recording equipment, which was not acting correctly; another was a finding that construction workers on site were not following all of the safety requirements. Several were related to corrective action and "cross−cutting" issues, said Dentel, in which a safety concern could "affect all areas of the plant," Dentel said.
Source: http://www.seacoastonline.com/news/hampton/03222005/news/712 24.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *March 22, Government Computer News* — **Free software available to help first responders identify chemicals.** The National Library of Medicine has created open source software for handheld devices to help first responders when they arrive at a hazardous materials incident, such as a chemical spill. The Wireless Information System for Emergency Responders (WISER) provides critical information about hazardous substances, including a substance's physical characteristics, any related health data, and containment and suppression information. WISER versions for handheld systems that run Palm OS and Pocket PC are available as free downloads. The National Institutes of Health agency plans to make a desktop PC version available this spring and is developing a Web version. "First responders in general, and Hazmat units in particular, must make decisions quickly in handling hazardous−materials incidents," said Dr. Jack Snyder, the library's associate director for specialized information services. Hazmat incidents are increasing, Snyder said, citing statistics from the Coast Guard's National Response Center. There were about 34,000 incidents reported last year.
Source: http://www.gcn.com/vol1_no1/daily−updates/35343−1.html

4. *March 21, Associated Press* — **Chemical spill causes evacuation at university.** Seven buildings on the New Mexico Tech campus in Socorro, NM, were evacuated Monday, March 21, after about a half−cup of bromine was accidentally spilled in one of the school's chemistry labs. Bromine has a noxious odor resembling chlorine and can irritate the nose, throat and eyes. No one was injured, but a hazardous materials team with the Socorro Fire Department responded while police evacuated buildings within a 1,000−foot perimeter. The spill was neutralized in about three hours, but the building remained closed until Tuesday morning as a

precaution.
Source: http://www.thenewmexicochannel.com/news/4305815/detail.html? rss=alb&psp=news

5. *March 21, Associated Press* — **Brewing company workers injured as a result of ammonia leak.** An ammonia leak at Portland Brewing Company in northwest Portland, OR, injured two workers and caused traffic delays Monday morning, March 21. Authorities said employees were in the process of changing out an ammonia tank when a valve jammed open sending two employees to the hospital, and forcing the evacuation of 15 people from the brewing company building. Nearby buildings were evacuated as well. Police also closed off several blocks around the brewing company as a safety precaution. Portland Fire and Rescue's Hazardous Materials team responded to the scene and set up equipment to analyze the leak. Ammonia is very toxic if inhaled and can be explosive in high concentrations. After the area was ventilated and the air tested by the Hazmat team, the brewing company was given permission to resume normal operations.
Source: http://www.kgw.com/news−local/stories/kgw_032105_news_ammonia_leak.15d2fc898.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *March 22, ComputerWeekly* — **UK banks on high security alert against key loggers.** City of London banks have been on alert since confidential warnings of a major high−tech theft were issued in December. The news emerged this week as police continued their investigation into an attempt by computer hackers to steal more than $400M from Japanese bank Sumitomo. Alerts were circulated to banks last year through a confidential banking information exchange, which warned of attempts by criminals to plant key logging software in critical bank systems. A second alert in January warned that banks should be on the lookout for hardware key loggers, which could be covertly inserted into desktop PCs to record passwords used for money transfers. "The most likely scenario is to have someone on the inside who gets a job in IT support, and to have that person go to the desktop, disable the anti−virus, install the key logger and re−enable the anti−virus," said Neil Barrett, an independent security consultant. He added that it is difficult to get key loggers through firewalls. John Meakin, group head of information security at Standard Chartered Bank, said banks often deployed push technology to ensure desktop systems are regularly reconfigured to their original settings, reducing the scope for tampering by staff.
Source: http://www.computerweekly.com/articles/article.asp?liArticleID=137452&liArticleTypeID=1&liCategoryID=6&liChannelID=22&liFlavourID=1&sSearch=&nPage=1

7.

March 21, InformationWeek — **Wireless security top concern for financial companies.** Secure and uncomplicated deployment of wireless technologies was the main focus of the second annual "Wireless On Wall Street" summit in New York on Monday, March 21. Business and technology professionals from banks, brokerages, and insurance companies attended the summit. While wireless technology can offer speed and agility, top challenges include dealing with the complexities of network integration, access points, and security. To effectively deploy wireless services, financial−services companies first have to plant a large−scale network that meets banking security measures. The real challenge lies in managing that wireless network once it has been deployed, said Geoff Smith, director of technical services at Aruba Wireless Networks. The need for a fully authenticated, encrypted wireless network remains high, summit attendees said. Financial−services companies are under constant pressure from customers and employees to implement wireless technology because of the convenience it offers. It's still unclear whether or not the financial−services industry is ready for widespread adoption of wireless, as security issues remain a major concern for most companies. But the consensus is that it's not enough just to secure the airspace and the networks surrounding financial−services companies. The physical infrastructure must be secured as well.
Summit Website: http://secure.imn.org/~conference/im/index2.cfm?sys_code=50322_TE_0005&header=on
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=159903610

[Return to top]

Transportation Sector

8. *March 22, Los Angeles Times (CA)* — **Pushing of trains gets new scrutiny.** Since Los Angeles's Metrolink commuter rail system opened in 1992, 15 passengers have died on Metrolink trains in three separate accidents −− all of them involving trains being pushed from behind by a locomotive instead of being pulled. Nationally, at least half a dozen accidents, killing 38 passengers and injuring almost 1,000, have occurred in the last decade involving trains being pushed. The widely accepted practice of pushing trains has gone on for decades in the commuter railroad industry, but since the deadly January 26 crash of a Metrolink train in Glendale, CA, it has come under intense new scrutiny. After long condoning the practice, federal regulators now say they are conducting a fresh review of the issue. Putting heavy locomotives at the rear of a train, some experts say, leaves passengers much more vulnerable in frontal crashes and may be particularly risky along routes shared with freight trains and in dense urban settings with frequent grade crossings. At 130 to 150 tons, locomotives provide passengers a large and hefty buffer in accidents. But putting the locomotives at the rear can make economic sense. By pulling trains one way and pushing the other, railroads avoid the costly and time−consuming practice of rearranging cars at the end of the line.
Source: http://www.latimes.com/news/local/la−me−metrolink22mar22,0,1384398.story?coll=la−home−headlines

9. *March 22, Associated Press* — **Comair flight attendants to vote on deal.** Comair has proposed cutting new workers' starting salaries, instead of freezing flight attendants' pay, so the airline can buy more planes and attract new business. The 1,000−member flight attendants' union will vote on the proposed deal through April 8. The local union's executive council has unanimously endorsed the deal, said Victoria Gray of the International Brotherhood of

Teamsters, which represents Comair's flight attendants. Comair, a Delta Air Lines Inc. subsidiary, is trying to recover from a nationwide Christmas Day shutdown that resulted from the failure of a computer system it uses to schedule flight crews. Comair officials said the system collapsed after a pre−holiday snowstorm caused numerous flight changes. The storm and related expenses cost Delta $20 million, including $5 million attributable to the Comair shutdown. The proposed deal also would guarantee the delivery of 35 new regional jets and increase the number of flight attendants by at least three percent to ensure adequate staffing. Gray said the concessions would save the company a substantial amount of money and would keep Comair's flight attendants the highest−paid in the regional industry.
Source: http://biz.yahoo.com/ap/050322/comair_flight_attendants_2.ht ml

10. *March 22, Associated Press* — **British Airways to increase fuel surcharge.** British Airways PLC said Tuesday, March 22, it is increasing its fuel surcharge in a bid to counter the effects of record high oil prices, following a similar move by Virgin Atlantic on Monday. British Airways said it is boosting the fuel charge on long haul one−way tickets by six pounds (US$11, euro8) to 16 pounds (US$30, euro23) a flight. The price of short haul tickets will increase by four pounds (US$7.50, euro5.60) to six pounds (US$11, euro8). British Airways said that the increase was unavoidable as it faced a 300 million pound (US$570 million, euro430 million) hike in its annual fuel bill. Prices have risen by about a third so far this year, fueled by a late cold snap across the world's largest energy consumer, the United States. They also have been underpinned by a weak dollar and rising global demand at a time when there is very little excess supply available.
Source: http://biz.yahoo.com/ap/050322/britain_airlines_fuel_surchar ges_1.html

11. *March 22, Associated Press* — **Task force to examine pipeline firm's inspections.** A federal agency has assembled a task force to examine how pipeline company Kinder Morgan Energy Partners inspects its lines and decides whether they need repair or replacement, an agency spokesperson said. It marked the first time the federal Pipeline and Hazardous Materials Safety Administration, formerly the Office of Pipeline Safety, has assembled a task force to examine safety practices along a multi−state pipeline, agency spokesperson Damon Hill said. "Kinder Morgan has had a few high−profile incidents recently," he said. "Any risks along the pipeline system could have an impact on public safety and the environment." "The federal government is certainly the right place for this issue to be considered," said Jay Thorne, a spokesperson for Texas−based Kinder Morgan. Thorne said yesterday the company reviewed and strengthened its inspection process after the July 2003 rupture near Tucson, AZ. Hill said his agency began assembling the multi−state task force last month. It will include the Arizona Corporation Commission, a state regulatory agency; the U.S. Environmental Protection Agency; and representatives from California, Nevada, New Mexico, Oregon and Texas. A report is expected by June, he said.
Source: http://www.tucsoncitizen.com/index.php?page=local&story_id=0 32205a5_pipelinesafety

12. *March 22, Newsday (NY)* — **Undocumented immigrant population soars.** The nation's undocumented immigrant population surged to 10.3 million last year, despite a sluggish economy and tighter border enforcement, a leading research group found in a report released on Monday, March 21. The number of illegal residents grew from 8.4 million in 2000, a 23 percent jump, according to the report by the Pew Hispanic Center in Washington, DC. "The border has

been the focus of federal efforts [to curb illegal immigration] and has not produced a reduction in flow," said Robert Suro, director of the center. Suro said the promise of earning a living beyond subsistence wages in their native countries remains a powerful motivation for many immigrants to defy the law. He added that the number of immigrants living in the United States illegally is growing as rapidly as in the late 1990s, even with a stalled U.S. economy and a post−September 11, 2001, border strategy that routs migrants to dangerous and isolated border crossings. The Pew Hispanic Center said it used federal Current Population Survey figures to count an increase of roughly 485,000 undocumented immigrants per year between 2000 and 2004. Report: http://pewhispanic.org/reports/report.php?ReportID=44
Source: http://www.newsday.com/news/local/longisland/ny−liimmi224186339mar22,0,109296.story?coll=ny−topstories−headlines

[Return to top]

Postal and Shipping Sector

13. *March 22, DM News* — **Postal Service looks to file across−the−board rate increase.** The U.S. Postal Service (USPS) is recommending to its Board of Governors that it file a rate case with the Postal Rate Commission for an across−the−board increase of five percent to six percent. The news was part of Postmaster General John E. Potter's keynote address Monday, March 21, at the National Postal Forum in Nashville, TN. Potter explained how the Civil Service Retirement System Funding Reform Act of 2003 helped the USPS avoid over−funding its Civil Service retirement obligation by reducing payments to the program. "These reduced payments, combined with $8.8 billion in cumulative cost savings, have allowed us to hold rates steady until 2006," Potter said. "Because the 2003 Civil Service Retirement System legislation also called for the establishment of an escrow account beginning in 2006 of $3.1 billion," Potter said, "use of the money in the escrow account is subject to the direction of the Congress. Were we to be able to use these funds for operating expenses, there would be no rate increase until 2007." The proposed rate increase funds the escrow requirement, he said. It would raise the cost of a First−Class stamp by two cents, with comparable percentage increases for other classes as well.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3226 5

[Return to top]

Agriculture Sector

14. *March 20, Fond Du Lac Reporter (WI)* — **Controlling Johne's disease constant struggle for dairies.** A recent survey showed that more than 22 percent of dairy herds in the U.S. are infected with the Johne's disease, which is costing the Wisconsin dairy cattle industry an estimated $54 million a year in reduced milk production. Dairy farmers with infected herds may be losing as much as $235 a year for every animal in their herd −− including those that don't have the disease, said Elisabeth Patton, of the Wisconsin Department of Agriculture, Trade & Consumer Protection. Johne's disease is a chronic infection of the lower small intestine of ruminants caused by an infectious bacterial organism most commonly found in manure of infected animals. The wall of the intestine thickens until it is unable to absorb nutrients,

essentially causing the animal to waste away. Patton said there is a way to control its spread through diligent management practices. “Culling alone won’t eliminate the infection. Instead we encourage producers and their veterinarians to develop a management plan that involves testing,” said Patton. Controlling Johne’s disease is a long−term effort. From the time producers begin implementing disease control strategies on newborn calves, there is a two−year window until the fruits of their intensive labor begin to pay off.
Source: http://www.wisinfo.com/thereporter/news/archive/local_202913 65.shtml

[Return to top]

Food Sector

15. *March 22, Minneapolis Star Tribune* — **Hormel to buy Lloyd's barbecue unit from General Mills.** General Mills Inc. said Monday, March 21, that it will sell its Lloyd's barbecue business to Hormel Foods Corp. The Golden Valley, MN, based food maker purchased Lloyd's Barbeque Co. in Mendota Heights, MN, in January 1999 from founder Lloyd Sigel. In February 1999, General Mills bought a California company, and the combined purchase price for both companies was $130 million. Lloyd's generated about $90 million in annual sales when it was acquired.
Source: http://www.startribune.com/stories/535/5305784.html

16. *March 21, U.S. Department of Agriculture* — **Egypt lifts ban on U.S. beef products.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns announced Monday, March 21, that Egypt is immediately resuming imports of U.S. beef and beef products from animals less than 30 months of age. "We are extremely pleased at the reopening of another important market for U.S. beef exports and anticipate that exports will quickly return to pre−BSE (bovine spongiform encephalopathy) trade levels," said Johanns. The agreement requires age and origin requirements under a USDA Agricultural Marketing Service Beef Export Verification (BEV) program. In 2003, Egyptian purchases of U.S. beef and beef products amounted to $30 million.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/03/0102.xml

17. *March 21, Food and Drug Administration* — **Smoked salmon recalled.** SeaSpecialties of Miami, FL, is voluntarily recalling "Mama's Sliced Smoked Nova Salmon" and "Mama's Smoked Salmon Nova Snacks" because they are contaminated with Listeria monocytogenes, an organism which can be serious and sometimes cause fatal infections. The recalled salmon was distributed on the east coast of the U.S. No illnesses have been reported as a result of this problem. The contamination was noted after routine testing by the Florida Department of Agriculture and Consumer Services revealed the presence of Listeria monocytogenes.
Source: http://www.fda.gov/oc/po/firmrecalls/seaspecialties03_05.htm l

[Return to top]

Water Sector

18.

March 21, Oregon Governor's Office — **Oregon governor announces statewide drought and fire strategy.** On Monday, March 21, Oregon Governor Kulongoski released a comprehensive strategy to address water shortages and potentially extreme wildfire danger, bringing state and local partners together to ensure that Oregon is prepared to respond to drought and fire emergencies this spring and summer. The Governor also called on the federal government to ensure that adequate resources are in place, including a full complement of crews and equipment to fight fires on federal lands in Oregon. “Oregon is experiencing the second driest winter on record, and that has serious implications for our economy,” Governor Kulongoski said. The Governor identified the Department of Water Resources, Oregon Drought Council, Oregon Department of Forestry and Office of Homeland Security as the primary drought and fire management agencies and directed them to: 1) monitor water and wildfire conditions and implement the state’s response; 2) update drought and fire planning activities throughout the state; 3) coordinate with local governments to assess local conditions and ensure effective processing of state and federal drought declarations and other state and federal assistance; and 4) coordinate with government at all levels, and with forest landowners, in sharing information about fire conditions and about the availability of firefighting resources.
Source: http://governor.oregon.gov/Gov/press_032105.shtml

[Return to top]

Public Health Sector

19. *March 22, Agence France Presse* — **Death toll from mystery hemorrhagic fever rises to 93 in Angola.** An outbreak of an unidentified hemorrhagic fever has claimed the lives of 93 people in northern Angola, Deputy Health Minister Jose Van Dunem said. Of the 101 cases reported in the Uige provincial hospital in northern Angola, 93 people have died and two have left the hospital without being properly discharged, said Van Dunem at a news conference. "We are engaged in an effort with the community to find the two patients who fled the hospital and to detect new cases," he said. The results of blood samples sent to Senegal showed that the mysterious outbreak was not due to yellow fever, dengue fever, the West Nile virus, the Crimean−Congo hemorrhagic fever, or rift valley fever, said Moises Francisco, a member of the Angolan technical team monitoring the outbreak in Uige. Angolan health officials have asked the U.S. Centers for Disease Control to conduct tests to determine whether the fever is caused by the Ebola virus.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=1&u=/afp/20050322/hl_afp/angolahealthfever_050322100845

20. *March 22, American Society for Microbiology* — **Food preservative neutralizes anthrax spores.** Nisin, a commonly used food preservative effectively neutralizes anthrax spores and could be used to decontaminate skin in the event of exposure. Researchers from Biosynexus Inc. report their findings Tuesday, March 22, at the 2005 American Society for Microbiology Biodefense Research Meeting. "Contamination of human skin with even a few spores may potentially disseminate disease beyond the initial area of attack," says John Kokai−Kun, a researcher on the study. "There is currently nothing specifically approved for decontaminating human skin of anthrax spores." Nisin is a natural antimicrobial peptide used as a preservative in heat−processed and low pH foods. It is derived from the controlled fermentation of the naturally occurring milk bacteria Lactococcus lactis. Kokai−Kun and his colleagues tested the

ability of nisin to neutralize spores of both anthrax and a related microbe, Bacillus cereus. Spores were pre−treated with nisin and then given variety of tests, including their ability to germinate and to cause disease in mice. While untreated spores in a control group were able to germinate and grow in culture and cause lethal infection in mice, the treated spores remained dormant and caused no apparent disease.
Source: http://www.innovations−report.de/html/berichte/biowissenschaften_chemie/bericht−42051.html

21. *March 22, American Society for Microbiology* — **Testing exhaled breath to detect infection.** Researchers from Johns Hopkins University are developing a novel method of testing exhaled breath to detect infection rapidly after potential exposure to a biological warfare agent. They report their findings Tuesday, March 22, at the 2005 American Society for Microbiology Biodefense Research Meeting. When exposed to disease causing organisms, cells in the body release proteins, called cytokines, to help the immune cells identify and fight the infection. Researchers theorized that cytokines might work their way up through the tissue until eventually they would be exhaled through water vapor in the breath, and could be captured and identified. In previous studies, researchers exposed pigs to different infectious agents and collected breath samples, which they condensed and ran through a mass spectrometer to test for cytokines and other proteins. They were able to detect a strong surge in cytokines in exhaled breath in as little as an hour, long before any visible symptoms appeared. Now that they have shown the concept of exhaled breath diagnostics to be viable, the next step is to move into human testing.
Source: http://www.news−medical.net/?id=8622

22. *March 21, USA Today* — **Health care shortages could feed a flu pandemic.** Scientists are racing against an evolving virus to prevent what could be millions of deaths from a flu pandemic, but what could trip them up is the simple lack of nurses and hospital beds, said Keiji Fukuda of the influenza branch of the U.S. Centers for Disease Control and Prevention. "No matter how good medical technology is, if we don't have health care workers to care for sick people and hospital beds to put them in, it's not a good situation," said Fukuda. Although not citing specifics, Fukuda says the best preparation for a flu pandemic is to strengthen basic public health systems by bolstering the vaccine supply and training more health care workers. Clinical trials of the first vaccine against H5N1, the so−called avian flu, have begun, but a vaccine can take six months to develop. The situation is bad enough in wealthy countries, but "90 percent of the world's population lives in countries with no vaccine production," he says. The U.S. has enough antiviral medications stockpiled to treat less than one percent of the population. With no medicine immediately available, Fukuda says, officials would rely on travel restrictions and quarantine to slow the spread of the virus. Conference: http://www.cdc.gov/nip/NIC/default.htm
Source: http://www.usatoday.com/news/health/2005−03−21−flu−pandemic_x.htm

23. *March 21, Associated Press* — **Asia flu cases may be undercounted.** The incidence of a particularly lethal variation of influenza in Southeast Asia is probably greater than has been reported so far, Keiji Fukuda, a flu expert at the Centers for Disease Control and Prevention said Monday, March 21. Since January 2004, an estimated 69 people, primarily in Vietnam, have contracted a type of influenza commonly referred to as bird flu. The fatality rate among those reported to have the disease is about 70 percent. But Fukuda said he suspects there are

more cases. "All infectious diseases have cases that are milder and cases that are more severe," said Fukuda, who spoke to medical officials at a conference on immunization. "All the cases we're seeing right now are the severe cases. There's got to be less severe ones out there." More information about avian influenza is available from the U.S. Centers for Disease Control and Prevention: http://www.cdc.gov/flu/avian/
Source: http://www.sci−tech−today.com/story.xhtml?story_id=31569

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24. *March 22, Inland Northwest Health Services* — **Global disaster exercise tests regional healthcare system.** Disaster and emergency response experts from nearly two dozen regional agencies in Spokane, WA, are ready to launch Ultimate Caduceus, a cooperative disaster exercise involving the Army, Air Force, Region 9 Homeland Security, Spokane Regional Health District, state and county emergency services and virtually every hospital in eastern Washington. The event takes place on Wednesday, March 23. The exercise is designed to test the ability of hospitals in eastern Washington to cope with a sudden influx of injured or wounded military people and their families. It revolves around the arrival of a C−17 aircraft from nearby McChord Air Force Base loaded with simulated victims of a major disaster in south Asia. After the exercise, organizers will analyze the outcome and define ways to improve regional emergency planning, preparation and response.
Source: http://www.prnewswire.com/cgi−bin/stories.pl?ACCT=109&STORY=/www/story/03−22−2005/0003239701&EDATE=

25. *March 22, Federal Computer Week* — **DHS pushes technology to first responders.** Officials in the Department of Homeland Security launched a test program Tuesday, March 22, to help smaller communities get commercially available cutting−edge technology to better handle terrorist threats. Through the Commercial Equipment Direct Assistance Program (CEDAP), the Office of State and Local Government Coordination and Preparedness will provide equipment and technical assistance to selected jurisdictions in accordance with their state's homeland security strategies. Under the program, first responders could receive a variety of technologies, including detection equipment for biological and chemical agents, night vision and thermal imaging devices, protective equipment, information−sharing and search software, analysis software and interoperable communications devices. The Responder Knowledge Base (RKB) is the official site for CEDAP applications. It is a national Website that provides first responders with information about equipment and related certifications, testing, standards, training, funding, reference material and publications, and further contacts. The competitive program is a direct assistance program and not a grant program. The initial application period will begin April 5 and last one month. RKB Website: http://www2.rkb.mipt.org/
Source: http://fcw.com/article88373−03−22−05−Web

26. *March 21, American Radio Relay League* — **Amateur radio to have role in mass casualty exercise.** Amateur Radio Emergency Service (ARES) members in Connecticut, New Jersey and several other states in the Northeast are preparing to take part in what's being characterized as the most comprehensive terrorism response exercise ever conducted in the U.S. Sponsored by the Department of Homeland Security and intended as a realistic test of the nation's homeland security system, the exercise−−TOPOFF 3−−gets under way Monday, April 4, and continues through the week. Connecticut Section Emergency Coordinator Chuck Rexroad, AB1CR, is in the process of lining up the 100 or so volunteers he estimates will be needed in the region for the mass casualty drill. "We're still looking for volunteers in all four types of positions needed," he said. ARES primarily will support the American Red Cross. Rexroad anticipates that ARES will be providing its traditional "backbone" communication support among Red Cross mobile feeding stations, the organization's temporary stationary facilities and other Red Cross units. ARES also will be ready to provide back−up communication support the Connecticut Office of Emergency Management, he said.
Source: http://www.arrl.org/news/stories/2005/03/21/101/?nc=1

27. *March 21, The Daily Freeman (NY)* — **Police unit to train for attack at high school.** On Tuesday, March 22, and Wednesday, March 23, police and members of a multi−agency response team in Saugerties, NY, will use Saugerties High School as a training ground where police and school administrators alike can practice their response to an attack. The drill is being held during spring break, when classes are not in session. The Emergency Response Team is made up of officers from several local police agencies trained and equipped to handle "active shooter" scenarios, hostage situations and other emergencies that call for military−style weapons and tactics. The team, along with similar units from the state police and Department of Environmental Protection, was charged with searching and securing the Hudson Valley Mall in Kingston, NY, last month following a shooting spree for which suspect Robert Bonelli Jr. of Saugerties has been charged. While the school drill was in the works prior to the mall incident, the attack heightened concern for school security, Saugerties Police Chief Gregory Hulbert said. "(Bonelli) said that if had been a Monday, he would have gone to a school," said Hulbert, referring to statements allegedly made by the mall shooting suspect after his arrest.
Source: http://www.dailyfreeman.com/site/news.cfm?BRD=1769&dept_id=74969&newsid=14186230&PAG=461&rfi=9

28. *March 21, Associated Press* — **Rural areas feel unprepared for attacks.** Rural health officials believe they are unprepared to respond to a possible terror attack on food supplies, nuclear power facilities or other targets. A survey of health officials in 26 states also found that most rural areas would not be prepared for a bioterror attack or have the resources to handle a surge of people fleeing urban areas under assault. The study, sponsored in part by the Harvard School of Public Health and the University of Pittsburgh, comes as the Department of Homeland Security is proposing awarding federal aid to states and localities based on the level of threats they face. Small and rural states fear such an approach would dramatically cut funding for their emergency responders. The survey listed a number of vulnerabilities unique to rural areas. It noted that water supply and energy sources, including nuclear plants, usually are based in rural communities. Militia activities are more common in rural areas, as is the potential for farm terrorism, the survey said, noting: "One cow down can paralyze an entire beef industry." Report: http://www.hsph.harvard.edu/hcphp/Conference_Proceedings.pdf

Source: http://abcnews.go.com/US/wireStory?id=601207&page=1

29. *March 18, Federal Computer Week* — **Vulnerability report on 2008 track.** An official from the Department of Homeland Security said last week a comprehensive assessment of the nation's preparedness and vulnerabilities will be ready in 2008. Matt Mayer, acting executive director of the Office of State and Local Government Coordination and Preparedness, said the National Preparedness Goal and National Preparedness Guidance will be released March 31. They will essentially establish measurable priorities and targets, assess the nation's preparedness to major events, prioritize needs, help states implement national strategies, and allocate resources. They will help state and local governments do a better job of first responder training and exercises, and align equipment standards and research and development needs, among other things. The goal is also to compare the level of preparedness they need with the level they have achieved, identify the gaps and then close them. Mayer said his office is responsible for implementing Homeland Security Presidential Directive 8 (HSPD−8), issued December 17, 2003, to help the nation develop a unified strategy to prepare state, local and tribal governments prevent, respond to and mitigate disasters, including terrorism. HSPD−8: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm
Source: http://www.fcw.com/article88346−03−18−05−Print

[Return to top]

Information Technology and Telecommunications Sector

30. *March 22, The Scotsman (Scotland)* — **British intelligence warns of possible cyber attack in UK.** International terrorists are training to launch cyber−terror attacks on Britain which could cripple vital economic, medical and transport networks, the government's counter−terrorism coordinator said Monday, March 21. Sir David Omand, one of the most senior members of the British intelligence community, said surveillance of suspected al Qaeda affiliates suggests they are working to use the Internet and other electronic communications systems to cause harm. Intelligence officials say that no matter how much the state does to prepare for cyber−terrorism, a great deal will rest on the willingness of the private sector to "harden" their systems against attack. Britain has not yet experienced genuine acts of cyber−terrorism, but Sir David said intelligence chiefs are in little doubt that the country must be ready for such an attack. The authorities' greatest fears about electronic attacks relate to the more exposed networks that make up what is known as "critical national infrastructure", many of which are in civilian hands. The global nature of the Internet means the threat from cyber−attacks is equally international, forcing British agents to work closely with nations they say they would often regard with suspicion or even hostility.
Source: http://thescotsman.scotsman.com/index.cfm?id=305582005

31. *March 22, vnunet (United Kingdom)* — **Hackers increasingly spreading malicious code via instant messaging.** Attacks using instant messaging (IM) as an unprotected backdoor in enterprises are reaching epidemic proportions, industry experts have warned. Analyst firm IDC Research said that the problem is leading to a sharp hike in highly sophisticated IM attacks that spread malicious code and worms directly into organizations without any end−user intervention. "Hackers and virus writers have realized that the next vulnerable area for attack within an organization is to spread malicious code via IM," said Brian Burke, research manager

for security products at IDC. Hackers are increasingly using IM as a vector for phishing scams and for so−called 'pharming' attacks, malicious redirects where thousands of IM users are persuaded to click on a link to a bogus, malware−infected Website. According to security firm Websense, incidents involving hackers using IM soared by 300 percent during the first quarter of 2005, compared with the fourth quarter of 2004. "Social engineering and vulnerabilities within IM client technologies are being used to gain access to hosts," said Dan Hubbard, senior director of security and technology research at Websense.
Source: http://www.vnunet.com/news/1162084

32. *March 21, Secunia* — **Java Web Start JNLP file command line argument injection vulnerability.** A vulnerability in Java Web Start, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an input validation error when handling property tags in JNLP files. This can be exploited to pass arbitrary command line arguments to the virtual machine by tricking a user into opening a malicious JNLP file. Successful exploitation can lead to the Java "sandbox" being disabled. The vulnerability has been fixed in J2SE releases 1.4.2_07 or later for Windows, Solaris and Linux.
Source: http://secunia.com/advisories/14640/

33. *March 21, Secunia* — **Subdreamer Light global variables SQL injection vulnerability.** A vulnerability in Subdreamer Light, which can be exploited by malicious people to conduct SQL injection attacks. Input passed to various global variables isn't properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Successful exploitation requires that "magic_quotes_gpc" is disabled. There is no vendor solution at this time.
Source: http://secunia.com/advisories/14652/

34. *March 21, InformationWeek* — **Presidential committee criticizes IT infrastructure security.** The President's IT Advisory Committee (PITAC) on Friday, March 18, released the results of a report, "Cyber Security: A Crisis Of Prioritization," criticizing the country's IT infrastructure as highly vulnerable to attack by terrorists and cybercriminals. "The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects," committee chair Marc Benioff and co−chair Edward Lazowska wrote in a February 28 letter to President Bush. This infrastructure includes the public Internet as well as power grids, air−traffic−control systems, financial systems, and military and intelligence systems, they add. The committee comprised of IT leaders and academia, makes four key recommendations to help curb security exposures and provide long−term IT infrastructure stability: increase federal support for fundamental research in civilian cybersecurity; intensify federal efforts to promote recruitment and retention of cybersecurity researchers and students at research universities; provide increased support for the rapid transfer of federally developed, cutting−edge cybersecurity technologies to the private sector; and, better federal coordination of cybersecurity R&D. Report:
http://www.itrd.gov/pitac/reports/20050301_cybersecurity/cyb ersecurity.pdf
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=159903541&t

35. *March 21, Government Computer News* — **New cybersecurity team meets this week.** The Office of Management and Budget (OMB) has created a task force that this week will begin figuring out how agencies can share cybersecurity functions. The team of senior IT managers will look at training, incident response, disaster recovery, contingency planning and how

agencies select security products. The March 23 kick−off meeting will start a six−month study. By September, the group must develop a business case for IT security functions that can be provided centrally by agencies or vendors. OMB wants the new cybersecurity task force to ferret out functions that, if shared or standardized, will mean quick and easy improvements across the government. Karen Evans, OMB's administrator for IT and e−government, said guidance from the task force's findings will be available to agencies for the fiscal 2007 budget cycle. OMB Website: http://www.whitehouse.gov/omb/
Source: http://www.gcn.com/24_6/news/35313−1.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: US−CERT has identified a recent increase of reported P2P incidents. P2P file sharing technology provides Internet users with the potential to share local files with a potentially unlimited number of other Internet users. As a result, the usage of P2P software may allow for sensitive data or personal information to be leaked from computer systems. Further, P2P may provide a vector for malicious code to be introduced into an enterprise environment.

Current Port Attacks

Top 10 Target Ports	22321 (wnn6_Tw), 445 (microsoft−ds), 3724 (−−−), 7674 (−−−), 135 (epmap), 139 (netbios−ssn), 53 (domain), 80 (www), 1026 (−−−), 1025 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

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

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

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

DHS/IAIP Disclaimer