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

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Washington Post reports the untiring efforts of hackers to cause serious damage to systems that feed the nation's power grid have heightened concerns that electric companies may have failed to adequately fortify defenses against a potential catastrophic strike. (See item 4)

- The Washington Post reports the Federal Trade Commission wants information brokers that collect and sell personal data to be subject to the same requirements to keep data secure as banks and other financial institutions. (See item 11)

- Shore Publishing reports the Department of Homeland Security is planning TOPOFF3 for April 4−8; it will simulate a coordinated terrorist attack on Connecticut and New Jersey, involving more than 10,000 participants from 200 international, federal, state, tribal, private, and local agencies. (See item 29)

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 12, Citrus County Chronicle (FL)* — **Federal agents make arrests at Crystal River complex.** Federal immigration agents arrested three contract workers at Progress Energy's Crystal River Energy Complex north of Crystal River, FL, Thursday, March 10, but the exact

charges were unknown, company spokesperson Rick Kimble said. Kimble said U.S. Immigration and Customs Enforcement (ICE) agents made the arrests. One of the three men arrested by ICE agents had given a false Social Security number to get a job with a contract company inside the Crystal River nuclear power plant. The arrival of federal immigration agents followed a tumultuous day for Progress Energy in which union leaders accused the company of allowing seven undocumented foreign workers to take jobs inside the nuclear power plant building as laborers. Two of the three men arrested were part of the seven initially accused of using false Social Security numbers, Kimble said. The seven men worked for Brock Specialty Services, a company that contracts with Progress Energy to provide maintenance laborers. Kimble said Brock Specialty Services is still "scratching its head" trying to figure out how its prescreening of employees failed. The Crystal River Energy Complex consists of a single nuclear unit and four fossil−fueled generators.
Source: http://www.chronicleonline.com/articles/2005/03/12/news/news 20.txt

2. *March 12, Associated Press* — **Organization for Petroleum Exporting Countries has reached output limit.** The Organization for Petroleum Exporting Countries (OPEC) has reached its production limit, and trying to stretch output by one million barrels per day isn't likely to lower oil prices, Algeria's minister for energy and mines said. Chakib Khalil said prices were high because of world economic growth −− particularly in the United States and China. “OPEC has reached its production limits. It doesn't have much production capacity,” he said at the opening of an industrial plant in the western town of Arzew, Algeria, according to newspaper reports on Saturday, March 12. “If it came to a crunch, it has capacity for one million barrels (more per day), and I don't think a production increase would influence the barrel price,” he said. Algeria is one of the 11 members of the OPEC.
Source: http://www.nytimes.com/aponline/business/AP−Algeria−OPEC.htm l?

3. *March 11, Reuters* — **International Energy Agency raises demand forecasts.** The International Energy Agency (IEA) said in its monthly Oil Market Report that estimated demand growth this year has been revised up by 290,000 barrels per day (bpd) to 1.81 million bpd, taking annual global consumption to 84.3 million bpd. The IEA has revised its estimate for 2005 world demand growth up by 500,000 bpd in the last three months, as synchronous growth in the Chinese and U.S. economies proves more resilient than expected to the impact of higher energy costs. "In real terms and relative to incomes oil prices are not yet at extreme levels," said Michael Lewis, head of commodities research at Deutsche Bank in a report. "When crude oil prices are deflated by G7 consumer price inflation, we find that oil prices would need to rise to $60 a barrel and $100 a barrel in current nominal dollars to be equivalent to the two price peaks during the 1970s," Deutsche Bank said. Report: http://omrpublic.iea.org/currentissues/full.pdf
Source: http://www.washingtonpost.com/wp−dyn/articles/A27002−2005Mar 11.html

4. *March 11, Washington Post* — **Hackers targeting U.S. power grid causes concern.** Hackers have caused no serious damage to systems that feed the nation's power grid, but their untiring efforts have heightened concerns that electric companies have failed to adequately fortify defenses against a potential catastrophic strike. The fear is that in a worst−case scenario, terrorists or others could engineer an attack that sets off a widespread blackout and damages power plants, prolonging an outage. Many electric industry representatives have said they are concerned about cyber−security and have been taking steps to make sure their systems are protected. However, Patrick H. Wood III, the chairman of the Federal Energy Regulatory

Commission, and others in the industry said the companies' computer security is uneven. "A sophisticated hacker, which is probably a group of hackers . . . could probably get into each of the three U.S. North American power [networks] and could probably bring sections of it down if they knew how to do it," said Richard A. Clarke, a former counterterrorism chief in the Clinton and Bush administrations. Clarke said government simulations show that electric companies have not done enough to prevent hacking. The biggest threat to the grid, analysts said, may come from power companies using older equipment that is more susceptible to attack.
Source: http://www.washingtonpost.com/wp−dyn/articles/A25738−2005Mar 10.html

5. *March 01, CBS 5 News (AZ)* — **Security leak at Phoenix utility.** An employee of Phoenix, AZ, utility APS was caught collecting social security numbers. A news investigation uncovered a contract worker for the power company who had pilfered 650 customer social security numbers. APS officials say they don't know why this person was collecting these numbers, but the county attorney's office is investigating.
Source: http://www.kpho.com/Global/story.asp?S=3017642

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *March 13, WITN (NC)* — **Chlorine leak forces evacuations.** Officials in Beaufort County, NC, say around 5:00 p.m. Saturday, March 12, a chlorine leak was discovered at a local water plant along Highway 33 near the city of Washington. Chlorine can be fatal if inhaled, so officials blocked off Highway 33 and a number of other roads in the area, and also evacuated a number of homes. It is unclear exactly what started the leak inside. An employee of the water plant was sent to the hospital because of the toxic fumes. That man was treated and released. Officials contained the leak, and re−opened Highway 33 around 10:15 p.m.
Source: http://www.witntv.com/news/headlines/1360422.html

7. *March 11, Herald−Dispatch (WV)* — **Medical school evacuated after chemical spill.** A chemical spill led authorities to evacuate more than 50 Marshall University medical students and staff Thursday, March 10, from an educational building at the Veterans Affairs Medical Center (VAMC) in Huntington, WV. A female student carrying a container of an agent known as TRI Reagent, which contains phenol, spilled some of it and suffered minor burns, according to Huntington Fire Department Deputy Chief Tim Provaznik. The student was taken to the adjacent VAMC for treatment. Provaznik said the spill occurred in an elevator about 1:30 p.m., and the entire building was evacuated as a precaution. The evacuation did not affect patients, staff and visitors at the VAMC, according to J.B. Finlay, its acting director. About 15 Huntington Fire Department (HFD) firefighters were on the scene assisting Marshall University and VAMC personnel. HFD Chief Greg Fuller and Mayor David Felinton also responded. Provaznik said the building likely would remain evacuated until a hazardous cleanup crew contacted by Marshall authorities arrived to contain the spilled chemical.
Source: http://www.herald−dispatch.com/2005/March/11/LNtop2.htm

8. *March 11, Hilltop (DC)* — **Mercury spill in power plant in Washington, DC.** Sixth Street in

Washington, DC, was temporarily closed Thursday, March 10, while emergency crews responded to a mercury spill at the Howard University Power Plant. According to Alan Etter, spokesperson for District Fire and EMS, an unspecified amount of mercury spilled in the plant, which supplies power to the whole university. The spill was reported to the fire department at 11:00 a.m. Thursday morning after a power plant employee tried to clean up the spill with paper towels. "The individual who did the cleaning has tested very high for mercury exposure. He has been decontaminated by Hazmat. In addition to the fire department, representatives from the Department of Health, the hazardous materials unit (Hazmat), and Campus Police officers were present.
Source: http://www.thehilltoponline.com/news/2005/03/11/Campus/Mercury.Spill.In.Power.Plant−892292.shtml

9. *March 10, Lake City Reporter (FL)* — **Chlorine leak shuts down Florida elementary school.** A chlorine leak at a Lake City, FL, water treatment plant Tuesday, March 8, forced officials to evacuate 550 students from Melrose Park Elementary School. Students were relocated to another middle school, according to Capt. Gary Laxton, spokesperson for the Lake City Police Department (LCPD). Dispatch received a 911 call concerning the leak at 1:16 p.m. Authorities from LCPD, Florida Highway Patrol and the Columbia County Sheriff's Office were able to evacuate the school and reroute area roads. Hazmat crews secured the leak and streets were reopened again by 2:06 p.m., Laxton said. No one was reported injured. The city is currently in the process of relocating the treatment plant. That project is expected to be completed within the next two years.
Source: http://www.lakecityreporter.com/articles/2005/03/10/news/top _story/news01.txt

10. *March 10, KERO (CA)* — **Chemical spill closes California road.** A chemical spill in Northwest Bakersfield, CA, sent two people to the hospital and left a major road shut down Wednesday, March 9. Hydrochloric acid spilled out of a tank at Slumburge Oil Company in Northwest Bakersfield, and two employees were overcome by hydrochloride fumes and received minor acid burns. In total, 5,000 gallons of acid were spilled. Part of Snow Road was closed for about an hour later that evening because of wafting fumes in the area. Fire crews finished their mop−up of the acid around 10 p.m. and reopened the road.
Source: http://www.thebakersfieldchannel.com/news/4272679/detail.htm l

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

11. *March 11, Washington Post* — **Federal Trade Commission head stresses data security.** Information brokers that collect and sell personal data on virtually every U.S. adult should be subject to the same requirements to keep data secure as banks and other financial institutions, the head of the Federal Trade Commission (FTC) told Congress Thursday, March 10. FTC

Chairman Deborah Platt Majoras told the Senate Banking Committee that better security is "an immediate need" in the largely unregulated database business. Financial institutions are required to take a number of steps to safeguard personal information, including having written security plans, employee training and technology to detect and respond to intrusions. Some data brokers double as financial institutions and are covered by existing law. But other big players, such as ChoicePoint Inc. and LexisNexis Group, both of which suffered recent breaches, are not. Majoras also encouraged Congress to consider a national law requiring that consumers be notified if their information has been obtained by hackers or fraud artists who penetrate the security of the data brokers.
Source: http://www.washingtonpost.com/wp−dyn/articles/A25691−2005Mar 10.html

12. *March 10, ZDNet (UK)* — **British banks in talks to fight identity theft.** Major British banks may soon tighten their security in a bid to protect customers from identity theft. RSA Security has been in discussions with all of the major UK banks about providing them with better security for their customers, the company said on Thursday, March 10. Although UK banks have been slow to take up increased security measures, RSA said they are now close to acting on identity theft. Last year, Howard Schmidt, the former cybersecurity advisor to the White House and chief security officer at eBay, called on online businesses to implement stronger authentication for their customers' security. Some banks in Norway are already taking the issue seriously by generating one−time tokens to authenticate the identity of customers.
Source: http://news.zdnet.com/British+banks+in+talks+to+fight+ID+the ft/2100−1009_22−5608885.html?part=rss&tag=feed&subj=zdnn

13. *March 10, TechWeb.com* — **Money motivates attackers.** According to a security intelligence firm, more than half the cyber−attacks conducted in 2004 were carried out by criminals interested in only one thing −− money. iDefense, a Reston, VA−based supplier of security intelligence, delved into its private database of more than 100,000 malicious code attacks to publish analytical findings publicly for the first time, said Ken Dunham, the company's director of research. Using that database, iDefense tallied a record 27,260 attacks in 2004. Over 15,000 of those, or some 55 percent, were specifically designed to covertly steal information or take over computers for criminal purposes, including identify theft and fraud, said Dunham. "This is a business," said Dunham, "with organized criminal groups around the globe continuing to mobilize resources to develop, sell, and launch Internet attacks." The future looks grim, said Dunham, with more and more attacks motivated by money. "We saw an exponential increase last year, and I see no evidence that that's slowing." iDefense also found that quantity wasn't the only thing increasing in malicious code. Attacks are now much more likely to breach traditional defenses such as firewalls, anti−virus software, and intrusion detection tools.
Source: http://www.internetweek.com/showArticle.jhtml?articleID=1594 00994

14. *March 08, Associated Press* — **U.S. court indicts three in alleged counterfeit credit card ring.** A U.S. federal grand jury indicted one Canadian and two other people Monday, March 7, for allegedly using counterfeit credit cards to ring up millions of dollars in fraudulent purchases in the United States and Canada between 1998 and 2001. The case "may be one of the largest counterfeit credit card rings ever discovered in North America," said Paul Morrissey, special agent in charge of the Secret Service's San Francisco field office. Prosecutors said the suspects stole credit card numbers and used the accounts to make purchases in San Francisco, New York, Philadelphia, Seattle, and the Canadian cities of Calgary and Vancouver between 1998

and 2001. Investigators allegedly found thousands of stolen account numbers from American Express, CitiBank, Wells Fargo, Capitol One Bank, and the Teachers Credit Union in Portland, OR.
Source: http://news940.dserv.ca/news.php?cat=8&id=b030802A

[Return to top]

Transportation Sector

15. *March 13, Star−Ledge (NJ)* — **Sick time crackdown at New Jersey airport.** A total of 210 security screeners, or nearly one−sixth of the force, have been disciplined at New Jersey's Newark Liberty International Airport during the past six months for abusing sick time, according to federal officials. The Transportation Security Administration (TSA) −− continuing a crackdown on the hub's chronic security lapses and absentee staffing problems −− has warned the screeners they have taken too many sick days. In addition, employees were told they must produce a doctor's note for future absences and that they may be fired for further violations. Newark, one of the airports breached by terrorists on 9/11, has the equivalent of 1,320 full−time screeners. Absenteeism has become a major contributor to the continuing security troubles and poor morale at Newark, current and former TSA employees said. Missed shifts often leave checkpoints short−handed, they say, and force screeners to work long shifts in areas where alertness and vigilance are essential. In addition to sick−time abusers, at least 17 other screeners and supervisors have been punished −− or have disciplinary actions pending, TSA officials said. One incident involves two staffers accused of pouring cleaning alcohol near an X−ray machine conveyer belt and lighting it afire, officials said.
Source: http://www.nj.com/news/ledger/index.ssf?/base/news−20/111069 3203216860.xml

16. *March 12, Sun−Sentinel (FL)* — **Canadian discount carrier Jetsgo ceases all operations.** An estimated 17,000 customers have been stranded in the United States and Canada when Jetsgo cancelled all flights on Friday, March 11. The airline had flights to 19 cities in Canada and 10 in the United States. It flew to several Florida cities including Orlando, St. Petersburg, and Fort Myers. Because Jetsgo is a Canadian airline, American carriers do not have to honor tickets. Difficult market conditions and competitive pressures, including high fuel prices, led the company to discontinue operations. Canadian regulators are also investigating Jetsgo over a January 20 accident at Calgary International Airport, where an airplane slid off the runway on landing. Transport Canada issued a notice Friday, March 11, giving the carrier 30 days to fix safety concerns raised in the inquiry. Last month, Jetsgo was ordered to fly at lower altitudes, where more fuel is consumed, because the carrier hadn't updated its flight manuals to comply with Canadian regulations, Transport Canada said. The airline had engine problems on two flights this month, including one March 4 that forced a plane to abort its takeoff in Toronto.
Source: http://www.sun−sentinel.com/business/local/sfl−zjetsgo12mar1 2,0,1769723.story?coll=sfla−business−front

17. *March 10, CNN* — **Continental faces Concorde probe.** Continental Airlines says it has been placed under investigation by a French magistrate judge for the suspected role played by one of its jets in the July 2000 crash of the supersonic Concorde that killed 113 people near Paris. A judicial investigation is normally a first step towards eventual criminal charges under French law. The decision followed an official report in December, which concluded that a metal strip

that fell off a Continental Airlines DC−10 and a fuel tank design fault led to the crash on July 25, 2000. The titanium strip caused a Concorde tire to burst, propelling rubber debris that perforated the supersonic jet's fuel tanks. Continental Airlines, based in Houston, issued the following statement on Thursday, March 12: "Continental Airlines was placed under investigation by the magistrate in today's hearing, but it is important to note that this is just the beginning of the investigation part of the proceeding. "We are confident that the evidence will ultimately show that Continental was not responsible for this tragic accident."
Source: http://www.cnn.com/2005/WORLD/europe/03/10/france.concorde/i ndex.html

[Return to top]

Postal and Shipping Sector

18. *March 13, Associated Press* — **New Jersey post office that sorted anthrax letters to reopen.** The Hamilton, NJ, post office is set to reopen Monday, March 14, three and a half years after handling anthrax−laced letters. Investigators have not determined who was responsible for the 2001 anthrax attacks, which killed four people across the country and sickened 17. There were five confirmed anthrax infections and two suspected cases in New Jersey, but no fatalities. Tests have not detected any remaining anthrax spores since the building was fumigated early last year with chlorine dioxide gas. The center was stripped to its bare walls and all furniture and mail−sorting equipment was replaced in a renovation that cost an estimated $80 million to $100 million. The building now has sensors to detect anthrax and other biological agents.
Source: http://www.suntimes.com/output/news/cst−nws−anthrax13.html

[Return to top]

Agriculture Sector

19. *March 13, Baltimore Sun (MD)* — **Maryland center to protect agriculture.** Maryland is stepping up its defense against terrorist threats, which could target farms or the nation's food supply. To help safeguard Maryland agriculture −− the state's largest industry −− the Maryland Emergency Management Agency announced Friday, March 11, the creation of the Center for Agro−security and Emergency Management. It's a coordinated effort by the University of Maryland's College of Agriculture and Natural Resources in College Park and the state Department of Agriculture "to respond rapidly to any terrorist attack" as well as "trying to protect against a disaster from happening," said Robert Halman, the center's coordinator. One of the center's primary missions is to coordinate communication and education to the public and to farmers. The center, based at College Park, would also work with federal and state agencies, along with the emergency operation centers in each county. Halman said the center would be plugged into such groups as the State Highway Administration "so that if we had to quarantine an area, we could do it very quickly." Halman said that staff members at five diagnostic laboratories scattered throughout the state are prepared to go to farms to take samples to determine whether there is an outbreak of any disease.
Source: http://www.baltimoresun.com/news/local/harford/bal−ha.farm13
mar13,1,769393.story?coll=bal−local−harford&ctrack=2&cset=tr ue

20. *March 10, Animal and Plant Health Inspection Service* — **Animal identification projects launch online.** States and tribes invested in the U.S. Department of Agriculture's new national animal identification system (NAIS) are increasingly offering online premises registration to ease their participants' first step toward getting involved. Identifying each location that allows for animal commingling is the foundation of the NAIS and must be established before animals can be tracked. For those who manage farms, ranches, auction barns, feedyards, exhibitions and fair sites, registering their premises is the first tangible action they can take to participate in the NAIS −− a system being created to help protect U.S. animal health. With more than a dozen projects now underway in over 30 states, USDA's Animal and Plant Health Inspection Service has seen the numbers of producers interested in learning more and taking part in the NAIS rise dramatically.
Source: http://www.aphis.usda.gov/lpa/news/2005/03/naisonline_vs.htm l

21. *February 14, Plant Management Network* — **Online soybean rust center now available.** The American Phytopathological Society (APS), in conjunction with the Plant Management Network (PMN) and other scientific organizations, is overseeing a new online soybean rust center. The site, co−organized by APS, the American Society of Agronomy, Crop Science Society of America, and Plant Health Initiative, is designed to serve as a clearinghouse of information on soybean rust. "This site is the one−stop center for information on soybean rust," said Doug Jardine, director of the APS Office of Public Affairs and Education. The site offers breaking news on soybean rust; links to featured soybean rust sites, including government, national, international, and university sites; and a soybean rust database that visitors can use to find information on the identification and management of soybean rust as well as links to university and extension sites. The site also offers a searchable soybean rust image database; soybean rust distribution maps; and soybean rust identification training materials. The site can be accessed at http://www.plantmanagementnetwork.org/infocenter
Source: http://www.plantmanagementnetwork.org/about/press/rustcenter /

[Return to top]

Food Sector

Nothing to report.

[Return to top]

Water Sector

22. *March 11, Government Accountability Office* — **GAO−05−253: Freshwater Programs: Federal Agencies' Funding in the United States and Abroad (Report).** As the world's population tripled during the past century, demand for the finite amount of freshwater resources increased six−fold, straining these resources for many countries, including the United States. The United Nations estimates that, worldwide, more than one billion people live without access to clean drinking water and over 2.4 billion people lack the basic sanitation needed for human health. Freshwater supply shortages—already evident in the drought−ridden western United States—pose serious challenges and can have economic, social, and environmental consequences. Multiple federal agencies share responsibility for managing freshwater

resources, but consolidated information on the federal government's financial support of these activities is not readily accessible. The Government Accountability Office (GAO) was asked to determine for fiscal years 2000 through 2004 how much financial support federal agencies provided for freshwater programs in the United States and abroad. For the purposes of this report, freshwater programs include desalination, drinking water supply, flood control, irrigation, navigation, wastewater treatment, water conservation, water dispute management, and watershed management. Highlights: http://www.gao.gov/highlights/d05253high.pdf
Source: http://www.gao.gov/new.items/d05253.pdf

23. *March 10, Associated Press* — **Liquid manure flows into two streams in Wisconsin.** A Wisconsin farmer's use liquid manure for fertilization on frozen ground has lead to a runoff of the fertilizer into surface waters during a recent thaw. Nearly a half−million gallons of liquid manure washed off the farm's field into two streams that flow into Lake Mendota. The farmer's name could not be released to the media, because the incident is still under investigation. The state's Department of Natural Resources (DNR) reported recently that there have already been five manure−related incidents this year, and it is suspected they were caused by the winter spreading of fertilizer. Those incidents resulted in two fish kills in southern Wisconsin streams, the release of 480,000 gallons of manure into Dorn Creek and the contamination of private drinking water wells in Dodge County, DNR officials said. Spreading liquid manure onto frozen farm fields is legal, but efforts are under way in parts of the state to prohibit the practice.
Source: http://www.gazetteextra.com/manurespill031005.asp

[Return to top]

Public Health Sector

24. *March 12, Reuters* — **Second nurse suspected to have bird flu in Vietnam.** A Vietnamese nurse who tended a bird flu patient with a colleague who has since tested positive for the virus has been hospitalized after showing symptoms of the disease, health officials said on Saturday, March 12. It was not clear yet if the 41−year−old female nurse caught the sickness from the patient or in another way, said an official at the health center of Thuy Luong commune, northern Thai Binh province. The nurse had provided care for a 21−year−old man who caught the virus last month after drinking raw duck blood. Her colleague, a 26−year−old male nurse who also tended the young man, tested positive for bird flu last week. The Thai Binh bird flu cluster has prompted an investigation into whether relatives and health workers caught the virus directly from infected patients.
Source: http://www.reuters.com/newsArticle.jhtml?storyID=7883649&typ e=worldNews

25. *March 12, Associated Press* — **Indiana reports whooping cough comeback.** Whooping cough cases rose to their highest number in four decades in Indiana last year due largely to the disease's spread among adolescents, health officials said. Indiana had 361 cases of whooping cough, or pertussis, in 2004 −− the most in any year since 1964, said Wayne Staggs, an epidemiologist with the Indiana State Department of Health. In 2003, the state recorded 103 cases. Staggs said about 75 percent of Indiana's cases were in people under the age of 20. Indiana isn't alone in whooping cough's resurgence. Last year, cases of the disease reached a 40−year high in the U.S. with about 20,000 cases nationwide.
Source: http://seattlepi.nwsource.com/national/apscience_story.asp?c

ategory=1500&slug=Whooping%20Cough

26. *March 12, Agence France Presse* — **WHO calls for full information on each bird flu case.** The World Health Organization (WHO) called for full disclosure of all information on each human bird flu case to prevent a global pandemic. "Full information on new cases, including those that may be closely related in time and place, is critical to ongoing assessment of the pandemic risk posed by the H5N1 virus," the WHO said. "Rapid field investigation of each new case is essential to ensure timely detection of clusters of cases occurring in family members or health care workers," WHO said. "Such cases can provide the first signal than the virus is altering its behavior in human populations and thus alert authorities to the need to intervene quickly." Since late 2003, WHO has registered a total of 69 cases, of which 46 were fatal: 33 in Vietnam, 12 in Thailand and one in Cambodia.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=2&u=/afp/20050312/hl_afp/healthfluvietnamwho_0503121726 20

[Return to top]

Government Sector

27. *March 11, Department of Homeland Security* — **Senate confirms Michael P. Jackson.** The U.S. Senate confirmed Michael P. Jackson by voice vote on March 10, as Deputy Secretary of the Department of Homeland Security. He was officially sworn in by Secretary Michael Chertoff and took office on March 11. Secretary Michael Chertoff issued the following statement: "I congratulate Michael Jackson for being confirmed with unanimous consent by the U.S. Senate as Deputy Secretary of the Department of Homeland Security. His management experience in public and private service will be extremely valuable to the Department and its vital mission. I thank Congress for acting quickly during the confirmation process and look forward to working closely with Deputy Secretary Jackson in the months ahead as the Department strives to enhance our capabilities and strengthen our nation's security."
Source: http://www.dhs.gov/dhspublic/display?content=4388

[Return to top]

Emergency Services Sector

28. *March 13, Gloucester County Times (NJ)* — **Emergency crews train for disasters.** Emergency responders in neon−green protective suits patrolled the campus of Gloucester County College in Sewell, NJ, on Saturday, March 12, testing chemicals and diagramming the layout of buildings as part of a drill. The exercise was part of a class offered by the Gloucester County Emergency Response Center and Underwood−Memorial Hospital EMS (emergency medical services) Academy. During the course of three days, 25 men and women from local police, fire and emergency medical services trained for a disaster involving weapons of mass destruction. On the third day, students will apply what they learned in a simulated, dirty bomb incident at the college's student center. Those in the course fulfill a classroom requirement that allows them to take part in "hot" training in Alabama offered by the Office of Domestic Preparedness. The week−long course there incorporates live agents like sarin.

Source: http://www.nj.com/news/gloucester/local/index.ssf?/base/news−8/111070530114920.xml

29. *March 11, Shore Publishing (CT)* — **Officials in Connecticut prepare for terror drill.** Southeastern Connecticut will be inundated with Secret Service agents, FBI agents and police officers for a security drill next month, along with role−playing reporters, bleeding and dying "victims," as well as hundreds of fire trucks, police vehicles and ambulances. The Department of Homeland Security (DHS) is organizing the drill, called TOPOFF3 (named for top officials), which will simulate a coordinated terrorist attack on Connecticut and New Jersey. The exercise, scheduled April 4−8, involves the United Kingdom, Canada and more than 10,000 participants from 200 international, federal, state, tribal, private and local agencies. The drill is meant to test top officials' ability to coordinate across all levels of government in the case of a wide−scale emergency. DHS has said the mock weapons of mass destruction to hit New London, CT, will be chemical in nature. Over in Waterford, CT, First Selectman Paul Eccard said residents can expect to see some activity near Millstone Power Station and possibly a number of vehicles being staged in places like the Crystal Mall and Waterford Speed Bowl. Local hospitals can expect to see an influx of patients on April 4, when most of the immediate emergency response is expected to occur.
Source: http://www.shorepublishing.com/archive/re.aspx?re=4a790342−ebce−495b−8285−41ce08659b4c

30. *March 10, Global Security Newswire* — **National security exercises test lawmakers.** Members of the House Homeland Security Committee went to Wye River, MD, Monday, March 8, to participate in the two separate tabletop exercises, which were chosen to represent what committee Chairman Christopher Cox (R−CA) called Wednesday, the two "most serious" threats to national security. The nuclear scenario involved a 10−kiloton nuclear bomb detonated at Grand Central Station after having been trucked there in a lead−sealed container. Cox said several "radical al Qaeda terrorist groups" claimed responsibility in the exercise, and initial casualty reports indicated 500,000 dead with a dramatic rise still expected. In playing out the nuclear scenario on the first day of their retreat, the House members focused on emergency response, health care, financial markets, prevention of further such attacks, cooperation with allies and the use of intelligence, according to Cox. The retreat's second day featured a smallpox and anthrax exercise modeled after the high−profile, U.S.−European exercise conducted last month, known as Atlantic Storm. During the bioterrorism exercise, legislators discussed the roles of international organizations, allocation of limited medical resources, public information and general infectious disease containment, Cox said.
Source: http://www.govexec.com/dailyfed/0305/031005gsn1.htm

31. *March 10, USA Today* — **Emergency Medical Services providers need training, equipment.** Although they represent a third of the nation's first responders, emergency medical services (EMS) providers have received only four percent of the $3.38 billion the Department of Homeland Security (DHS) gave out for emergency preparedness in 2002 and 2003. A report, "Emergency Medical Services: The Forgotten First Responder," released Friday, March 11, by New York University's Center for Catastrophe Preparedness and Response also found that more than half of the country's 900,000 emergency medical technicians (EMTs) and paramedics have received less than one hour of training in dealing with biological and chemical agents and explosives since the 9/11 terrorist attacks, and 20% have received no such training. DHS'

largest grant program is for overall emergency preparedness, and that money is doled out to the states, which then must decide how to spread it around among emergency responders. Sen. Susan Collins (R−ME), chair of the Senate Homeland Security and Governmental Affairs Committee, introduced a bill last week that will create a federal committee to help guide EMS providers through the complex grant process and make sure federal preparedness money is well−spent. Report: http://www.nyu.edu/ccpr/events/20050311−000124.html
Source: http://www.usatoday.com/news/nation/2005−03−10−ems−lax_x.htm ?POE=NEWISVA

32. *March 08, Loudoun Times−Mirror (VA)* — **MCI's emergency response team stages drill.** Last week at MCI's Ashburn, VA, headquarters, employees participated in a hazardous materials emergency response drill. The telecommunications company's Emergency Response Incident Team (MERIT) is made up of 32 MCI employees from around the country, trained to repair damage to MCI's communications equipment and network in the event of a natural disaster, terrorist attack or large−scale accident. Twice a year, the team conducts a training exercise to test members' ability to respond to different emergency scenarios. This drill centered on the scenario of a fire that sends chemical gases into the air and forces all MCI employees to evacuate the premises. In last week's simulation, MERIT's duties included testing the air quality to determine when it was safe for MCI employees to return to work and repairing any equipment damaged by corrosion from airborne chemicals. According to MERIT's team leaders, the drills not only keep members well−trained for real emergencies but also help them establish relationships with other emergency responders around the country.
Source: http://www.timescommunity.com/site/tab1.cfm?newsid=14107686&BRD=2553&PAG=461&dept_id=506039&rfi=6

[Return to top]

Information Technology and Telecommunications Sector

33. *March 11, SecurityFocus* — **MySQL AB MySQL multiple remote vulnerabilities.** MySQL is reported prone to multiple vulnerabilities that can be exploited by a remote authenticated attacker. MySQL is reported prone to an insecure temporary file creation vulnerability. It is also prone to an input validation vulnerability that can be exploited by remote users that have INSERT and DELETE privileges on the 'mysql' administrative database and may be leveraged to load and execute a malicious library in the context of the MySQL process. It is reported that the vendor has addressed these vulnerabilities in MySQL versions 4.0.24 and 4.1.10a. Users should consult http://dev.mysql.com/downloads/ for availability of these downloads.
Source: http://www.securityfocus.com/bid/12781/info/

34. *March 10, Associated Press* — **Singapore tops survey of tech readiness.** The United States is no longer first in making the best use of information and communications technology, a new study says. It dropped to fifth place this year and Singapore is now tops. Singapore's ranking in the so−called "networked readiness index" was based on several factors, including quality of math and science education and low prices for telephone and Internet services, said the World Economic Forum report. The United States' drop from first place last year "is less due to actual erosion in performance" than to the improvement of other countries, the report said. Report: http://www.weforum.org/site/homepublic.nsf/Content/Global+Co

mpetitiveness+Programme%5CGlobal+Information+Technology+Repo rt
Source: http://www.washingtonpost.com/wp−dyn/articles/A23545−2005Mar 10.html

35. *March 10, Computerworld* — **Companies turn to secure instant messaging to meet privacy concerns.** With the use of instant messaging (IM) on an upswing, companies concerned about security, regulatory and privacy issues are sometimes turning to secure IM solutions that allow only authorized users access to IM – while stopping others from sending instant messages. Available software provides businesses with control and administration of all IM activity by their workers, including dynamic detection and routing of IM use on the network, and prevention of unauthorized IM usage. Lawrence Orans, an analyst at Gartner Inc., said IM technology tools can now increase security because they allow businesses to set policies on permitted IM usage. While some companies do little to monitor their employees' IM use, the potential for viruses and network attacks will make it more important that they pay attention to potential problems, he said. "It will increasingly become risky to look the other way," Orans said. Another analyst, Robert Mahowald at IDC Inc., warned that there are still pitfalls to instant messaging, even with the use of secure applications. "You've significantly increased your chances of blocking [viruses and other problems] by having a secure IM solution in place," Mahowald said. "But it doesn't completely solve the problem."
Source: http://www.computerworld.com/softwaretopics/software/groupwa re/story/0,10801,100298,00.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: Several vulnerabilities were identified in MySQL, which may be exploited by local attackers to execute arbitrary commands or obtain elevated privileges. For more information, please visit the following link: http://www.k−tik.com/english/advisories/2005/0252

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 20525 (−−−), 135 (epmap), 53 (domain), 80 (www), 1026 (−−−), 139 (netbios−ssn), 6346 (gnutella−svc), 1027 (icq), 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

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.