Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 02 March 2005

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

Daily Highlights

- The Financial Crimes Enforcement Network has released an interim adjustment to its strategic plan that reflects the organization's growing role in detecting terrorist financing. (See item 4)
- KGTV reports Mexican officials and U.S. federal authorities from San Diego are investigating a border tunnel connecting a luxurious Mexicali residence to neighboring Calexico, California. (See item 13)
- The U.S. Centers for Disease Control and Prevention has released recommendations for policymakers who are seeking to create mandatory public reporting systems of healthcare−associated infections. (See item 20)

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, State and Local: 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 01, East Valley Tribune (AZ)* — **Utility says it is working to avoid power outages.** Arizona Public Service (APS) officials said Monday, February 28, they are making progress in implementing recommendations from two consultants on how to avoid power disruptions such as afflicted Phoenix's electric system last summer. At a hearing in front of the Arizona Corporation Commission, APS president Jack Davis said the utility is upgrading technology, replacing key components, building concrete fire walls at substations and enlarging

maintenance staff to reduce the chances of the same types of failures happening again. The consultants recommended that additional redundant relays be installed to protect the system in the event of line faults, improvement in communications protocols, improved diagnostic tools to detect equipment damage and other improved maintenance practices. APS officials said they have either adopted those recommendations or will adopt them.
Source: http://www.eastvalleytribune.com/index.php?sty=37196

2. *February 28, New York Independent System Operator* — **New York Independent System Operator releases final report on the 2003 blackout.** The New York Independent System Operator (NYISO) on Monday, February 28, released its "Final Report on the August 14, 2003 Blackout." The final report states that New York did not initiate or contribute to the system disturbance. The report concludes that the control area operated by the NYISO was functioning normally and with appropriate reserves just prior to the blackout, which affected 50 million people in the United States and Canada. The NYISO's operators had less than 10 seconds to respond to the sudden and severe power surge, which originated outside New York. The report confirms there was no time for human intervention. Full power was restored to New York within 30 hours. "The electric industry has learned a great deal in the past 18 months, but without national mandatory reliability standards that are strictly enforced, our chances for another major system failure will continue," said NYISO President and CEO William J. Museler. The NYISO report details how the power problems in the Midwest created a severe power surge that entered New York from the Midwest through Pennsylvania, and continued into the Ontario system. Within seconds, power lines connecting New York and PJM tripped offline. Report: http://www.nyiso.com/topics/articles/news_releases/2005/blackout_rpt_final.pdf
Source: http://www.nyiso.com/topics/articles/news_releases/2005/pr_nyiso_final_blackout_report%20_2_28_05_release.pdf

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *March 01, Computer Weekly* — **Bancorp guards its e−mail from attackers.** Online bank Bancorp Bank claims to have eliminated Website downtime and improved the efficiency of its e−mail communications after installing information technology to protect its systems against directory harvest attackers. The bank, which provides managed online banking services for more than 60 organizations, put in protection systems last year after a series of attacks by

spamming groups disrupted e−mail communications with its 8,000 banking customers. Bancorp discovered its systems were being bombarded by messages from hacking groups attempting to identify valid e−mail addresses on the company's systems for resale to spammers. Pete Chiccino, chief security officer at Bancorp, said, "This caused a slowdown in mail delivery because we were trying to process the invalid messages. It took us offline while we waded through 30,000 e−mails. One time it was an entire day."
Source: http://www.computerweekly.com/articles/article.asp?liArticleID=137021&liFlavourID=1&sp=1#

4. *February 28, Financial Crimes Enforcement Network* — **Financial Crimes Enforcement Network releases strategic plan.** The Financial Crimes Enforcement Network (FinCEN) announced on Monday, February 28, the release of an interim adjustment to its Strategic Plan for Fiscal Years 2003 – 2008. This adjustment to the regular strategic planning cycle covers Fiscal Years 2006 −2008 and reflects the organization's growing role in detecting terrorist financing and a recent organizational realignment. The Plan outlines four strategic goals, one management goal, and related objectives and strategies. The plan also discusses strategic challenges and how success will be measured. "The work we do is critical not only to the safety of our financial system but to our country's national security as well," said William J. Fox, FinCEN's Director. "The Financial Crimes Enforcement Network needs to be sophisticated, agile and creative in assessing and responding to the risks posed by criminals and terrorists. This Strategic Plan sets forth a blueprint on how we will marshal our assets to achieve this vital mission," said Fox. Plan: http://www.fincen.gov/strategicplan2006_2008.pdf
Source: http://www.fincen.gov/qnstrategicplan.pdf

[Return to top]

Transportation Sector

5. *March 01, nj.com* — **Airport screener seized for brass knuckles.** An off−duty security screener at Newark International Airport was arrested Sunday night when he tried to pass a set of brass knuckles through an airport X−ray machine, authorities said yesterday. Darren Castro, 22, of Jersey City, NJ, was arrested by Port Authority of New York and New Jersey police after he attempted to take the prohibited item through the checkpoint at Terminal C, said Lou Martinez, a spokesperson for the Port Authority which operates the airport. Possession of brass knuckles is a fourth−degree crime in New Jersey, punishable by a fine and up to 18 months in jail.
Source: http://www.nj.com/news/ledger/jersey/index.ssf?/base/news−8/1109688652277191.xml

6. *March 01, Associated Press* — **Logan needs security personnel for new terminal.** Logan International Airport in Boston, MA, needs to hire 125 security screeners to staff the rebuilt Terminal A, which reopens in two weeks. George Naccara, head of agency operations in Boston, is confident he will be able to fill all the jobs because of the agency's training office and recruiting center in Chelsea, MA. "It's a challenging job because we are asking these people to do two things at the same time: provide a high level of security and a high level of customer service," Naccara said. The $475 million rebuilt Terminal A at Logan is the first terminal at a major American airport to be designed and built for the post−9/11 era. It has wider

checkpoint waiting areas and a baggage screening area with networked computers that can be operated by fewer screeners. There are about 800 screeners at Logan who have to check about 12 million passengers per year as well as screen about 15 million pieces of luggage. They find about 11,000 banned items per years, from guns and knives, to cologne bottles shaped like sticks of dynamite, to cigarette lighters made to resemble handguns.
Source: http://www.lowellsun.com/business/ci_2590423

7. *March 01, Associated Press* — **Kentucky airport security officials find gun in luggage.** Security officials at Louisville International Airport retrieved a firearm from the luggage of a police trainer, Bob Stewart. The handgun was found as he was passing through a security checkpoint on his way to Florida on February 24. Stewart said he took the gun to work earlier that day to practice at the police firing range. He said he forgot the gun was in his bag. Both the FBI and the Transportation Security Administration are investigating the incident, airport spokesperson Rande Swann said. Federal authorities have not yet said whether he would be charged.
Source: http://www.thelouisvillechannel.com/news/4242218/detail.html

8. *March 01, KCRA Channel (CA)* — **Sacramento airport security screener accused of theft.** A security screener in Sacramento has been arrested after being accused of stealing money from a passenger's luggage. Transportation Security Administration investigators say they caught Forrest Foote, 55, on surveillance video stealing cash from a golf bag. "An operation was put into play, and he was essentially caught and immediately terminated," said TSA spokesperson Jeff Holmgren. Foote now faces charges of petty theft as well as possession of drugs.
Source: http://www.thekcrachannel.com/news/4242634/detail.html

9. *March 01, Government Technology* — **Connecticut governor urges strengthening driver's licenses issuing process.** On Friday, February 25, Governor M. Jodi Rell urged the Connecticut Senate transportation committee to move forward with legislation she proposed to strengthen and improve systems used to issue driver's licenses, motor vehicle registrations, and identity cards in order to prevent fraud and abuse. Rell said, "This bill make its clear that we are ready to use all available resources and the latest technology to carefully verify the identity of anyone who applies for a driver's license, motor vehicle registration or an identity card. These documents are used for identity and law enforcement purposes and it is critical we take all proper precautions in issuing them." The Governor has also directed the Department of Motor Vehicles to implement a comprehensive license−fraud prevention plan that includes the issuance of temporary licenses and identification cards while detailed background checks are completed and stronger measures are used to verify the identify of individuals before permanent documents are issued.
Source: http://www.govtech.net/magazine/channel_story.php?channel=26 &id=93189

10. *March 01, CTV (Canada)* — **Smoke forces evacuation of Toronto−bound plane.** More than 300 passengers traveling from Pakistan to Canada were forced off their plane at a British airport, after smoke was spotted coming from beneath the Pakistan International Airlines Boeing 777. The plane had landed at England's Manchester Airport on Tuesday, March 1, to refuel for its journey from Karachi to Toronto. According to airport authorities, the plane suffered a small fire, "connected to overheating," as it was taxiing. Although it posed no threat to the facility, the incident was enough to close the airport for 15 minutes, while the 323

passengers and 12 crew of flight PK 789 evacuated the plane via emergency chutes. Describing the incident, airline spokesperson Samina Parvez said when the control tower spotted smoke under the plane's left wing, it issued an alert. The chief of the airline's engineering department said the incident was likely connected to a greasing problem with the plane's wheels. "This is the fifth incident of similar fire with our Boeing 777 and the matter was reported to the manufacturer," Mukhatar A. Qazi said.
Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1109682010858_142/?hub=TopStories

11. *March 01, Reuters* — **Continental reaches deal with unions.** Continental Airlines announced its major unions have tentatively agreed to wage and benefit concessions worth $500 million a year, in a deal the airline had said was key to its survival. The Houston−based airline, struggling with record−high jet fuel costs, had warned it risked running out of cash if it did not strike this deal by February 28. The airline said concessions by pilots, flight attendants, mechanics and dispatchers would take effect at the end of March, adding that the airline would distribute 10 million shares of common stock to employees as part of the deal. Continental is the last of the six major traditional, or legacy, carriers to seek pay and benefit cuts or work−rule changes, though the wage cuts come on top of about $1 billion in costs the airline has slashed in other areas. Continental −− squeezed by energy prices and competition −− had losses of over $1.5 million a day in January. Even with the concessions, Continental faces a tough year as long as oil prices stay high, said Mike Miller, a consultant at the Velocity Group. "With oil at $52 a barrel all airlines are going to have to be creative with financing to accomplish their goals," he said.
Source: http://www.cnn.com/2005/TRAVEL/03/01/bt.continental.unions.r eut/index.html

12. *March 01, Los Angeles Times* — **Jet flies on with one engine out.** A British Airways jumbo jet lost power in an engine on takeoff from Los Angeles International Airport (LAX) last month, but the pilot elected not to make an emergency landing for repairs, deciding instead to continue the 5,400−mile, transatlantic flight to London on the remaining three engines, officials said Monday, February 28. The incident began as British Airways' Flight 268 lifted off from LAX at 8:45 p.m., on February 20. It carried 351 passengers. Because of unfavorable winds and inefficiencies resulting from the engine loss, the Boeing 747−400 burned more fuel than anticipated, and the pilot was forced to cut the nonstop flight short and land in Manchester, England, the airline said. Aviation officials in England and the United States are looking into the incident, and two retired jumbo−jet pilots now serving as air safety consultants said they were amazed at the decision to continue the flight. "We are concerned," said Laura Brown, a spokesperson for the Federal Aviation Administration. She said officials were determining whether any federal regulations were violated.
Source: http://www.latimes.com/news/local/la−me−britair1mar01,0,1554462.story?coll=la−home−local

13. *February 28, KGTV (CA)* — **Border tunnel discovered in upscale neighborhood.** Federal authorities from San Diego are investigating a border tunnel discovered by Mexican authorities over the weekend. The tunnel connected a luxurious Mexicali residence to neighboring Calexico, CA, officials with the Mexican Federal Attorney General's Office said. Inside the passageway, investigators discovered lighting and ventilation equipment, a closed−circuit security system, hydraulic machinery and various tools. The finding led agents to believe that

the tunnel was presumably used for drug trafficking. A middle section of the tunnel was initially discovered in the United States early Friday by U.S. Border Patrol agents checking for tunnels in a residential area of Calexico, the newspaper reported. It is the third tunnel found in Calexico in the past 15 months. "This is an ongoing criminal investigation..." said Lauren Mack, a spokesperson for U.S. Immigration and Customs Enforcement in San Diego. Source: http://news.yahoo.com/news?tmpl=story&u=/kcci/20050301/lo_kg tv/2604859

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

Nothing to report.
[Return to top]

Food Sector

14. *February 28, Food Safety and Inspection Service* — **Pork products recalled.** LeBlanc's Cajun Boudin and Food Company, Inc., a St. Amant, LA, establishment, is voluntarily recalling approximately 1,120 pounds of cooked pork products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Monday, February 28. The pork products were produced on February 14, 2005, and distributed to retail stores in the New Orleans and Baton Rouge areas. The problem was discovered through routine FSIS sampling. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease. Source: http://www.fsis.usda.gov/News_&_Events/Recall_008_2005_Relea se/index.asp

15. *February 28, Food Safety and Inspection Service* — **Ground beef sampling shows substantial E. coli decline.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) Monday, February 28, released data showing a 43.3 percent drop in the percentage of E. coli O157:H7 positive ground beef regulatory samples collected in 2004 compared with the previous year. Of the 8010 samples collected and analyzed in 2004, 0.17 percent tested positive for E. coli O157:H7, down from 0.30 in 2003, 0.78 in 2002, 0.84 in 2001, and 0.86 in 2000. Between 2000 and 2004, the percentage of positive samples in FSIS regulatory sampling has declined by more than 80 percent. There were six recalls related to E. coli O157:H7 in 2004 compared to 12 in 2003 and 21 in 2002. In 2002, FSIS ordered all beef plants to reexamine their food safety plans, based on evidence that E. coli O157:H7 is a hazard reasonably likely to occur. Plants were required to implement measures that would sufficiently eliminate or reduce the risk of E. coli O157:H7 in their products. FSIS personnel then began to systematically assess those food safety plans for scientific validity and to compare what was written in plant Hazard Analysis and Critical Control Point (HACCP) plans to what was taking place in daily

operations.
Source: http://www.fsis.usda.gov/News_&_Events/NR_022805_01/index.as p

[Return to top]

Water Sector

16. *February 28, Associated Press* — **New York appeals court says farm manure rules not protecting water.** A federal appeals court Monday, February 28, agreed with environmentalists that federal clean water rules established in 2003 were not protecting the nation's waters from the manure pollution of large farms. The Second U.S. Circuit Court of Appeals in New York said it agreed with environmentalists who claimed in lawsuits that the rules failed to provide meaningful review of plans developed by farms to limit the pollution. The court said the rules imposed in February 2003 by the Environmental Protection Agency (EPA) were arbitrary and capricious and did "nothing to ensure" that each large farm was complying with requirements to control the pollution. Its ruling requires the EPA to make changes so it can ensure compliance by farms with the Clean Water Act. Farms can generate millions of tons of manure each year, which carries potentially harmful pollutants −− including pesticides, bacteria, viruses, trace elements of arsenic and compounds such as methane and ammonia −− to water sources.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−fac toryfarmlawsui0228feb28,0,1873159.story?coll=ny−region−apnew york

[Return to top]

Public Health Sector

17. *March 01, Times (United Kingdom)* — **United Kingdom to stockpile drugs against bird flu pandemic.** The United Kingdom (UK) is to buy almost 15 million courses of a powerful antiviral drug to protect the country against a pandemic of the bird flu virus. The drug purchase will be enough to treat one in four of the UK population, the level recommended by the World Health Organization. If a pandemic broke out there would be a delay until an effective vaccine could be developed −− during which time the anti−viral drug could be used to control the illness and alleviate its effects. The Swiss drugs company Roche will supply 14.6 million courses of Tamiflu over the next two financial years, with 7.3 million courses available by the end of 2005−06 and the rest as soon as possible during the next financial year.
Source: http://www.timesonline.co.uk/article/0,,2−1506055,00.html

18. *March 01, Reuters* — **Vietnam confirms more bird flu infections.** A 35−year−old Vietnamese woman and a 14−year−old girl, both in the north of the country, have contracted bird flu, which has killed 47 people in Asia. The Lao Dong newspaper said Tuesday, March 1, the woman was taken to hospital on February 24 and tests confirmed Monday, February 28, she had the virus. A laboratory researcher said tests on the other patient, the 14−year−old girl, also confirmed she had the virus that had also infected her 21−year−old brother. Her brother has been in critical condition and on a respirator after a traditional drink of duck blood before the Lunar New Year festival last month, officials said.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=7771726

19. *March 01, New York Times* — **U.S. germ research policy is protested by scientists.** Scientists sent a petition on Monday, February 28, to the director of the National Institutes of Health (NIH) protesting what they said was the shift of tens of millions of dollars in federal research money since 2001 away from pathogens that cause major public health problems to germs the government fears might be used in a bioterrorist attack. The scientists say grants for research on the bacteria that cause anthrax and five other diseases that are rare or nonexistent in the U.S. have increased fifteen fold since 2001. Over the same period, grants to study bacteria not associated with bioterrorism have decreased 27 percent, the petition said. The letter was signed by 758 scientists who have received grants from the institutes or have served on panels helping to distribute them in the fields of bacteriology and mycology. Anthony Fauci, the director of National Institute of Allergy and Infectious Diseases, which controls 95 percent of the institutes' biodefense spending, said the petition's signers were mistaken. Fauci said the $1.5 billion a year the administration decided to spend on biodefense research was new money and not taken from existing NIH programs. He said much of the biodefense research should also help protect against natural emerging disease threats.
    Source: http://www.nytimes.com/2005/03/01/politics/01petition.html?

20. *February 28, U.S. Centers for Disease Control and Prevention* — **Committee offers guidance to states for reporting of healthcare−associated infections.** The U.S. Centers for Disease Control and Prevention's (CDC) Healthcare Infection Control Practices Advisory Committee (HICPAC) Monday, February 28, released recommendations for policymakers who are seeking to create mandatory public reporting systems of healthcare−associated infections. To date, four states −− Illinois, Pennsylvania, Missouri, and Florida −− have passed laws requiring hospitals to publicly report healthcare−associated infections. And an additional 30 states are moving toward mandatory public release of this information. While HICPAC concluded there is currently not enough evidence to determine whether mandatory public reporting of healthcare−associated infections will reduce infection rates, the advisory committee recommended that states implementing public reporting should strive to gather meaningful infection control data and use nationally recommended infection control measures. To provide consumers and healthcare facilities with the best information, HICPAC recommends that states that are developing public reporting systems be sure to use established public health surveillance methods; involve people with infection control expertise in the process; and track practices that prevent infections. CDC estimates that each year nearly two million patients in the U.S. contract infections in hospitals and about 90,000 of these patients die as a result of their infection.
    Source: http://www.cdc.gov/od/oc/media/pressrel/r050228.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

21. *March 01, Agence France Presse* — **Interpol tackles bioterror threat.** Police chiefs gathered at an Interpol conference this week were urged to battle harder against the menace of an attack with biological agents, feared to be the weapon of the future for terrorists. The international community must "redouble its efforts" against the bio−terrorist threat, French Interior Minister Dominique de Villepin told more than 400 delegates from at least 120 countries at the Interpol headquarters in Lyon. Villepin suggested improving international cooperation in the struggle, notably by creating a common database. He called for efforts to improve the security of category "P3" and "P4" laboratories working with potentially dangerous germs or biological agents, as well as the creation of an international monitoring and coordination centre. For Europe, Villepin proposed a "European reaction plan against a biological attack" and a European Union update on reserves of vaccines so that each country can know the nearest country to turn to in case of emergency. Topics to be covered in the conference include the threat of bio−agents and toxins, forensic challenges, and the U.S. anthrax attacks. Conference: http://www.interpol.int/Public/BioTerrorism/Conferences/1stG lobalConference.asp
Source: http://www.afp.com/english/news/stories/050301174247.sdtbhbc c.html

22. *March 01, Associated Press* — **Natural disasters on coasts concern the National Oceanic and Atmospheric Administration.** Coastal area growth poses environmental and economic challenges to local governments, the National Oceanic and Atmospheric Administration (NOAA) said in a report on coastal population trends released Tuesday, March 1. Whether it's tsunamis on the West Coast or hurricanes and other storms in the Atlantic and Gulf Coasts, rising populations complicate evacuations and make emergency response more complex, officials said. Vertical evacuation −− moving people upstairs in taller structures −− is a possibility in some areas, like those at risk of tsunamis, said Richard Spinrad, director of NOAA's National Ocean Service. Vertical evacuation has also been proposed in areas such as New Orleans where hurricanes or floods could threaten large urban areas with limited evacuation opportunities. Overall, the new study said 153 million people live in coastal counties, an increase of 33 million since 1980. The area is expected to add another 12 million by 2015. Report: http://www.oceanservice.noaa.gov/programs/mb/supp_cstl_popul ation.html
Source: http://news.yahoo.com/news?tmpl=story&u=/ap/20050301/ap_on_s c/coastal_population_1

23. *March 01, Eufaula Tribune (AL)* — **Emergency response team runs mock drill.** Members of the Barbour County Emergency Response Team put their knowledge to the test Friday, February 25, with a mock hazardous waste situation. The team, comprised of firefighters, law enforcement and other emergency service personnel from all over Barbour County, AL, has been studying the proper way to clean up and manage a chemical spill. Friday's mock run was a culmination of a week of classroom training. The equipment, which includes hazardous waste protective gear, a command post trailer and a truck to haul the equipment, was purchased by the Department of Homeland Security for Barbour County. The train the Barbour County Emergency Response Team used was the DuPont CAER car. The car travels across the country for emergency personnel to practice. It has valves and fittings for hands−on training. Air and water are used to simulate leaks and releases of hazardous materials during training exercises, according to the DuPont pamphlet. The train visits are free to communities that wish to participate in the training experience.
Source: http://www.zwire.com/site/news.cfm?newsid=14055972&BRD=2235& PAG=461&dept_id=439676&rfi=6

24. *February 28, The Arizona Republic* — **Teens get a chance at firefighting.** The Fire Science Program at Metro Tech High School in Phoenix, AZ, recently partnered with the Bureau of Land Management (BLM) to enhance student's fire−suppression training. Touted as the first partnership between the federal agency and a high school, students complete about 15 hours of physical training, plus crew simulations and advanced wild−land firefighting techniques, in addition to the schools' structured firefighting and emergency medical training. Graduates 18 or older qualify for summer stints with the BLM, typically earning from $5,000 to $15,000 depending on the number of wildfires. Last year, all of the Phoenix school's graduates were placed in BLM summer stints, traveling as far as Alaska for the jobs, said Ed Metzger, head of the firefighting program. This summer an additional ten could make the cut, according to Dean Fernandez, BLM fire crew lead.
Source: http://www.azcentral.com/news/articles/0228wildland28.html

25. *February 27, Student Life (MO)* — **Students play dead for medics.** Emergency Support Team (EST) medics at Washington University in St. Louis, MO, conducted a disaster drill Sunday, February 27, attending to roughly 25 students with injuries ranging from third degree burns and broken legs to smoke inhalation and swollen abdomens. According to Disaster Drill Co−Chair Erica Kane, a drill is conducted each semester to train EST medics and make sure protocols are effective. After the medics assess their wounds and heart rate, victims are tagged with colors that represent differing levels of injury. Eventually, medics will carry them out of the building on backboards if they are unable to walk themselves. Students participating in the event received makeup beforehand to make their injuries look realistic. EST Field Director Matt Vogt noted that the point of this drill was to learn how to package patients correctly, whether on backboards, stretchers or simply carrying them out. Medics also focused on how to run a situation when there are many patients.
Source: http://www.studlife.com/news/2005/02/28/News/Students.Play.Dead.For.Est−879249.shtml

[Return to top]

Information Technology and Telecommunications Sector

26. *March 01, Federal Computer Week* — **Departments of Homeland Security and Justice work on XML model to help share information.** Department of Homeland Security (DHS) and Department of Justice officials have a new partnership to enhance development of an Extensible Markup Language (XML) model that could save federal, state, local and tribal agencies billions of dollars as they improve their computer systems to share information with one another. Officials said this represents a significant step in broadening the use of the Global Justice XML Data Model, which was started about three years ago, across the federal government. It could mean future partnerships with other departments, such as Transportation and Health and Human Services, and the intelligence community, which used the model as the basis for a schema to share the terrorism watch list. XML is essentially an open standard or translator that systems can use to communicate with one another. Development of the core model would ensure long−term stability of the model and ensure that early efforts in its use are not wasted. The information−sharing initiative is called the Collaboration on Objects for Reuse and Exchange.

Source: http://www.fcw.com/fcw/articles/2005/0228/web−dhsdoj−03−01−0 5.asp

27. *February 28, CNET News* — **NIST releases final security guidelines.** A final version of security guidelines designed to protect federal computer systems and the information they hold was released Monday, February 28, by the National Institute of Standards and Technology (NIST). The guidelines will serve as a road map for federal agencies in meeting mandates set by the Federal Information Security Management Act (FISA). Government agencies will be required to have certain security controls, policies and procedures in place. At the heart of the initiative is an effort to protect the confidentiality, integrity and availability of all federal information systems that are not part of the national security system. The security controls in the new NIST guidelines span 17 key areas, ranging from user identification to authentication to risk assessment. Guidelines: http://csrc.nist.gov/publications/nistpubs/800−53/SP800−53.p df
Source: http://news.com.com/NIST+releases+final+security+guidelines/2100−7348_3−5593256.html?tag=nefd.top

28. *February 28, Secunia* — **Debian bsmtpd arbitrary command injection vulnerability.** A vulnerability has been reported in bsmtpd, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to lack of sanitation of email addresses. This can be exploited to execute arbitrary commands. Original Advisory and updates available: http://www.debian.org/security/2005/dsa−690
Source: http://secunia.com/advisories/14412

29. *February 28, iDEFENSE* — **Mozilla Firefox and Mozilla Browser out of memory heap corruption design error.** Remote exploitation of a design error in Mozilla 1.7.3 and Firefox 1.0 may allow a remote attacker to cause heap corruption, resulting in execution of arbitrary code. The vulnerability specifically exists in string handling functions, such as nsCSubstring::Append. Certain functions, such as nsTSubstring_CharT::Replace() fail to check the return value of functions which resize the string. A failed exploitation attempt may result in the browser crashing. There is no solution at this time.
Source: http://www.idefense.com/application/poi/display?id=200&type=vulnerabilities&flashstatus=false

30. *February 28, K−Otik Security* — **phpBB administrator session handling critical security update.** Two vulnerabilities were reported in phpBB, which may be exploited by attackers to determine the installation path or bypass certain security features. The first problem resides in the "autologinid" (includes/sessions.php) variable and could be exploited by malicious users to gain administrator rights. The second flaw resides in the "viewtopic.php" script, and could be exploited to disclose the webroot path. Update to version 2.0.13: http://www.phpbb.com/downloads.php
Source: http://www.k−otik.com/english/advisories/2005/0212

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: Microsoft released an out of cycle patch for Windows XP Service Pack 2 and Windows Server 2003 systems to address an issue that can cause a computer to stop responding if certain firewall or anti−virus programs are installed on the machine. The following knowledgebase article discusses the patch: http://support.microsoft.com/kb/887742
To obtain the patch, please visit the following link:
http://windowsupdate.microsoft.com
The FBI is also reporting that emails claiming to be from its 'Internet Fraud Complaint Center' are actually virus−laden scams. The FBI never sends out unsolicited emails and asks that if you receive one of these bogus emails, please report it to the Internet Crime Complaint Center at http://www.ic3.gov.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 139 (netbios−ssn), 1025 (−−−), 1026 (−−−), 1027 (icq), 80 (www), 53 (domain), 137 (netbios−ns), 25 (smtp) 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