Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 11 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 federal officials are hastening efforts to close off the final stretch between Southern California's Otay Mesa port of entry and the Pacific Ocean, in a canyon known as Smuggler's Gulch, which they contend is a national security risk. (See item 8)
- The Honolulu Advertiser reports the number of late−season flu cases reported in Hawaii soared during February, reaching nearly one in every 10 physician visits during the middle of the month −− and it may not yet have reached its peak. (See item 18)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *March 10, Associated Press* — **New Yucca Mountain schedule may be ready by summer.** A top Yucca Mountain official says a new timeline for opening the national nuclear waste repository should be ready this summer. W. John Arthur said on Thursday, March 10, at a Nuclear Regulatory Commission (NRC) conference in Rockville, MD, that the new schedule will include dates for critical decisions about transportation, licensing and operations. Project officials are now looking at 2012 as the opening date, however, Arthur says that really depends on the Environmental Protection Agency and on the project budget. The NRC will decide if the Department of Energy can build at Yucca Mountain, 90 miles northwest of Las Vegas, NV. Source: http://www.kesq.com/Global/story.asp?S=3054270

[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

2. *March 10, Vnunet.com* — **Businesses worldwide revealing data to drive−by hackers.** The explosion of wireless networks is leaving global businesses wide open to 'drive−by hacking' and other security risks, experts have warned. According to research released on Thursday, March 10, more than a third of businesses worldwide with wireless networks are open to abuse from hackers and criminals in the street or a neighboring building. The study, commissioned by RSA Security, estimated that wireless networks in Europe's financial capitals alone are growing at an annual rate of 66 percent, and more than a third of businesses remain unprotected from this type of attack. The research was based on studies in the business centres of New York, San Francisco, London and Frankfurt. Some 38 per cent of businesses in New York, 35 per cent in San Francisco, 36 per cent in London and 34 per cent in Frankfurt were at risk from drive−by hacking. The study also revealed that many businesses had failed to take even basic security precautions such as reconfiguring default network settings. This means that wireless network access points could still be broadcasting valuable information that could be used by potential hackers and assisting them in launching an attack.
   Source: http://www.vnunet.com/news/1161837

3. *March 10, CIO Today* — **Credit card flaws fuel online fraud bonanza.** Today's credit cards are vulnerable to online fraud because of fundamental design flaws, industry experts warned Thursday, March 10. According to Forrester Research, the provision of all security and other functionality on a single physical card makes it intrinsically unsafe. Ivan Remsik, senior analyst for financial services at Forrester, warned that, as long as multiple technologies use or reside on the same physical plastic entity, fraud is set to rise. The analyst firm also warned that card fraud is increasingly moving online. Remsik argued that "something clearly needs to be done" to reduce the ease with which card−not−present fraud can be perpetrated, in particular online. Forrester indicated that various types of online scams targeting the consumer are on the increase, both technical, such as Trojans, and nontechnical, such as phishing. The analyst firm believes that fighting this threat effectively must combine technical and nontechnical responses from financial services institutions, and potentially others such as ISPs.
   Source: http://www.cio−today.com/story.xhtml?story_title=Credit−Card−Flaws−Fuel−Online−Fraud−Bonanza&story_id=31104

4. *March 02, Times Online (UK)* — **Fraudsters target charities through Web bank details.** Charities in the United Kingdom (UK) risk having their bank accounts emptied by fraudsters using a devastatingly effective new scam, the UK Charity Commission has revealed. Criminals are exploiting the fact that charities often publish their bank account details on the Internet in the hope that making their accounts easily accessible will encourage people to donate. Instead, fraudsters copy the bank details and use them to set up bogus standing orders to steal funds from charities. Because legitimate signatures are needed to set up standing orders, the Charity Commission believes that the crooks have used the charities' annual reports and accounts to make forgeries. Andrew Hind, the chief executive of the commission, said: "This is a particularly worrying scam because it requires no contact with the charity, leaving charities with no opportunity to become suspicious at any point of contact." Fraudsters are using bank account details, forged signatures and the charity's registration number to set up wire transfers to overseas companies.
   Source: http://business.timesonline.co.uk/article/0,,9075−1506364,00 .html

[Return to top]

Transportation Sector

5. *March 10, CNN* — **Pilots group says aviation security programs lacking.** The Coalition of Airline Pilots Associations is giving dismal grades to aviation security, saying, "gaping holes" remain almost four years after the September 11, 2001, terror attacks. The group gives failing or near−failing grades to the government and airlines for most aspects of security, from the airport perimeter to the cockpit, concluding that security measures deserve a grade point average of about 1.1. The best grades go to two areas that have received a lot of attention. Airport baggage screening received a grade of "B." Cockpit doors also received a "B," although the group noted that strengthened cockpit doors are not mandated in cargo planes of foreign carriers. The "Aviation Security Report Card" was compiled by the Coalition of Airline Pilots Associations, a trade association of five pilot unions that represent 22,000 pilots. The Coalition of Airline Pilots Associations is smaller, and it has tended to be more critical of government and industry than the Air Line Pilots Association, which represents 64,000 pilots at 41 airlines in the United States and Canada. About $5.6 billion of the Transportation Security Administration's $5.8 billion annual budget is directed toward aviation security. Report can be downloaded in PDF format from this site: http://www.capapilots.org/aviation_security.html
   Source: http://www.cnn.com/2005/TRAVEL/03/10/aviation.security/index .html

6. *March 10, Agence France Presse* — **Baggage handlers quarantined in Portugal after contact with suspect powder.** Eight baggage handlers at Lisbon's international airport have been quarantined after being exposed to a white powder that leaked from a suitcase from a U.S. plane, causing their eyes and throat to become irritated. The mysterious substance was found in capsules which fell out of a bag which had just been unloaded late Wednesday, March 9, from a Continental Airlines plane that arrived from Newark, NJ, it was reported Thursday, March 10. The baggage handlers received first aid at the airport, Portugal's busiest, and will remain at home until tests on the powder determine what it is, the president of their STHA union told national news agency Lusa. Preliminary tests on the white powder carried out at the airport ruled out anthrax. Firefighters searched the plane and submitted it to a chemical wash before it returned to the U.S. Airport officials were not immediately available for comment.

Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=3&u=/afp/20050310/hl_afp/portugalusairtransport_0503101 50827

7. *March 10, Department of Transportation* — **Amtrak reform plan to aid inter−city rail.** Department of Transportation Secretary Mineta says the federal government would be a "full partner" in plans to boost inter−city passenger rail service in Missouri and across the Midwest under the Bush Administration's proposal to reform Amtrak Mineta was in St. Louis, MO, on Thursday, March 10, as part of a nationwide campaign to reaffirm President Bush's commitment to reform of the nation's passenger rail system just weeks after the Administration unveiled a budget that proposed an end to taxpayer subsidies for Amtrak. He said Missouri's plans to improve passenger rail would benefit from the President's reform proposal "by letting the federal government match your infrastructure investments dollar for dollar," instead of spending all of its money every year on Amtrak. The proposal, Mineta said, would establish a 50−50 federal match for state investments in passenger rail infrastructure, like stations, trains and track, and open passenger rail service to competition. The plan would give states more control over schedules and routes and free Amtrak to focus on running trains, he added. He said Amtrak has problems partly because it runs money−losing routes and regularly diverts cash away from repairs to cover operating losses.
Source: http://www.dot.gov/affairs/dot4505.htm

8. *March 10, Washington Post* — **Entry point in San Diego considered a possible security risk.** With recent revelations by the Department of Homeland Security that al Qaeda operatives are looking to the Mexican border as a way to infiltrate the United States, federal officials have hastened efforts to close off the final stretch between Otay Mesa −− California's largest commercial land border port, a community within the City of San Diego −− and the Pacific Ocean, in a canyon known as "Smuggler's Gulch." They contend that the area is a national security risk. The U.S. House recently approved immigration legislation, introduced by Rep. F. James Sensenbrenner Jr. (R−WI), that includes provisions to complete the fencing. Built with recycled−steel landing mats donated by the military, the primary fence runs a jagged line along the southern U.S. border, about 10 miles from the Pacific Ocean to Otay Mesa. To close the gap in the second fence, a little less than three miles inland from the Pacific Ocean, Border Patrol officials plan to level off several of the mesas that surround the area and backfill the half−mile−wide canyon known as Smuggler's Gulch to create a 175−foot earthen berm.
Source: http://www.washingtonpost.com/wp−dyn/articles/A21825−2005Mar 9.html?sub=AR

9. *March 09, WFMY News (NC)* — **Illegal immigrant workers arrested at North Carolina airport.** Federal immigration officials arrested nearly 30 workers at an airport maintenance facility on Tuesday, March 8. More than two−dozen illegal immigrants working in a high−security area of Piedmont Triad International (PTI) Airport in Greensboro, NC, now face deportation. Federal agents arrested 27 workers at the Timco facility at PTI on Tuesday for using counterfeit documents to get their jobs. Timco is a company that does maintenance on both passenger and cargo aircraft. Federal agents say they have no reason to believe the workers at Timco were involved in any terrorist activity. But some airport passengers were shocked over the arrests. The investigation, called "Operation Tarmac" is part of a nationwide effort by immigration officials to target employers and unauthorized workers that have access to sensitive areas at airports. So far federal agents have apprehended more than a thousand unauthorized immigrant workers across the nation.

Source: http://www.wfmynews2.com/news/local_state/local_article.aspx ?storyid=37469

[Return to top]

Postal and Shipping Sector

10. *March 10, Detroit Free Press (MI)* — **Two courthouses cleared after anthrax scare.** Courthouses in downtown Detroit and Bloomfield, MI, were evacuated Wednesday, March 10, after employees opened envelopes containing white power and notes suggesting they contained anthrax, authorities said. Both were determined to be hoaxes. The Frank Murphy Hall of Justice, which houses the Wayne County Circuit Court criminal division and prosecutors' offices, was evacuated after an employee of Judge Timothy Kenny opened an envelope about 3:30 p.m., said Darryl Fordham, chief of staff for the Wayne County Sheriff's Office. Fordham said a note inside the envelope stated the powder was anthrax, but officials later said it appeared to be part of a hoax. The contents of the letter, as well as the identity of the sender, remained under investigation. Earlier in the day, local and federal authorities responded after an employee of 48th District Court in Bloomfield Township opened an envelope about 10:50 a.m. that contained white powder, police said. The courthouse was reopened about 1:30 p.m.
Source: http://www.freep.com/news/locoak/anthrax10e_20050310.htm

11. *March 10, KOLD−TV (AZ)* — **Detecting anthrax in the mail.** Every authorized piece of mail for southern Arizona comes through the Tucson processing and distribution center for the U.S. Postal Service. That's about eight million parcels any given day −− an average of 500,000 letters alone. Tucson's central office last week installed a biohazard detection system. The goal is to identify any presence of Anthrax. After letters are dropped off at the distribution center, a machine processes them and cancels out their stamps. What's new is a pinch−point...where each envelope is compressed and an air sample is taken. The sample is absorbed into a sterile liquid, then checked for anthrax. If there's a positive match, an alarm will sound, and the building will be evacuated. By summer's end, 283 postal districts nationwide are expected to have detection technology in place.
Source: http://www.kold.com/Global/story.asp?S=3056480&nav=14RTXJH8

[Return to top]

Agriculture Sector

12. *March 10, Associated Press* — **Georgia to protect food supply from terror, natural disaster.** Georgia is creating a statewide network of 3,500 emergency workers, farmers, and veterinarians who will help protect the nation's food supply from terrorist attacks and natural disasters. The program could become a model for other states because its aim is to not only protect consumers but also Georgia's $42 billion agricultural industry from economic ruin, according to Lee Myers, who heads the state's agroterrorism committee. By June 2006, Myers' committee plans to train 3,500 key people across the state to identify and then respond to any kind of agricultural emergency. In the case of agroterrorism, for example, veterinarians would be on the lookout for unexpected symptoms in animals and farmers would report any signs of unusual plant sicknesses. County agricultural agents were trained at the University of Georgia's

Rural Development Center. The agents will train the emergency workers, farmers, and veterinarians in their communities. Speakers at the training classes told the agents that terrorists could include religious fanatics, unstable people, animal−rights activists, and ransom seekers using inexpensive, low−tech gear. Disruptions of the food supply, even from natural occurrences, can also have grave psychological and political consequences, speakers said.
Source: http://www.insidebayarea.com/businessnews/ci_2603864

13. *March 09, Associated Press* — **Fungus enlisted to combat invasive weed.** The plant disease Turkish rust fungus has been enlisted to eliminate the yellow starthistle, an invasive thorny weed plaguing Monterey, CA, rangeland. "This is the very first fungus, the very first plant pathogen, to be fully approved as a biological control agent for use in the mainland U.S.," said Dale Woods, a plant pathologist with the California Department of Food and Agriculture. California released the rust at test sites in 20 counties last year and releases are expected to double this year, officials said.
Source: http://www.theksbwchannel.com/news/4268931/detail.html

14. *March 09, Associated Press* — **Partnership hopes to map soybean genetic code.** Agribusiness company Monsanto has teamed with a biotechnology company and the U.S. government in a bid to unlock the genetic code of soybeans, hoping to supply breeders with technology that makes the crop more resistant to disease and drought. Monsanto, Genaissance Pharmaceuticals Inc. and the U.S. Department of Agriculture (USDA) seek to map DNA markers in soybeans, creating a detailed molecular genetic map. That information then will be freely available to U.S. soybean breeders and geneticists on federal databases and in scientific journals, creating the first publicly available map of its kind. "What we learn from this research will be critical in our search for additional insights into ways to improve the characteristics, production rates and disease resistance of a variety of field crops, including soybeans and other plant species," said Gerald Vovis, executive vice president of Genaissance.
Source: http://abcnews.go.com/Business/wireStory?id=566783

15. *March 08, Government Accountability Office* — **GAO−05−214: Homeland Security: Much Is Being Done to Protect Agriculture from a Terrorist Attack, but Important Challenges Remain (Report).** U.S. agriculture generates more than one trillion dollars per year in economic activity and provides an abundant food supply for Americans and others. Since the September 11, 2001, attacks, there are new concerns about the vulnerability of U.S. agriculture to the deliberate introduction of animal and plant diseases (agroterrorism). The Government Accountability Office (GAO) examined the federal agencies' roles and responsibilities to protect against agroterrorism, the steps that the agencies have taken to manage the risks of agroterrorism, and the challenges and problems that remain. The U.S. Department of Agriculture (USDA) and other federal agencies have taken a number of actions. The agencies are coordinating development of plans and protocols to better manage the national response to terrorism, including agroterrorism. However, the U.S. still faces challenges that limit the nation's ability to respond effectively to an attack against livestock. USDA would not be able to deploy animal vaccines within 24 hours of an outbreak as called for in a presidential directive. There are also management problems that inhibit the effectiveness of agencies' efforts to protect against agroterrorism. Since the transfer of agricultural inspectors from USDA to the Department of Homeland Security in 2003, there have been fewer inspections of agricultural products at the nation's ports of entry.

Source: http://www.gao.gov/docsearch/abstract.php?rptno=GAO−05−214

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

16. *March 10, Associated Press* — **Washington prepares to cope with drought.** Washington Governor Christine Gregoire, responding to predictions of a severe drought in Washington, declared a statewide drought emergency on Thursday, March 10. Gregoire directed the state's Emergency Drought Committee to gear up an emergency command center, track and coordinate responses by state agencies and make sure state resources reach needed areas. Gregoire also ordered the National Guard to prepare to combat wildfires this summer and requested that the state legislature boost drought−related appropriations by an additional $8.2 million. As the Pacific Northwest girds for the worst drought in 28 years, precipitation is at or near record lows across the state. Mountain snowpack averages are running nearly 75 percent below average, and many rivers are at or near record lows for this time of year. The water shortage hurts farmers, hydroelectric power production, fish production, irrigation, and other sectors of the region's agribusiness economy, in addition to creating concern that there will be an unusually bad fire season. Meteorologists blame a weak El Nino, which brought unusually mild weather to the region in January, February, and now March. Water managers say the situation hasn't been this bad since 1977.
Source: http://seattlepi.nwsource.com/local/215396_drought10ww.html

[Return to top]

Public Health Sector

17. *March 10, Agence France Presse* — **Malaria cases underestimated by half.** At least half a billion cases of malaria occur each year, 50 percent more than is estimated by the World Health Organization (WHO). So say an international team of epidemiologists, who believe the WHO's malaria estimates are so disastrously wide of the mark that a global attempt to control the mosquito−borne disease by 2010 is at threat. WHO estimates more than a million people are killed by malaria each year, and at least 300 million acute cases of the disease occur annually, 90 percent of them in sub−Saharan Africa. The new study suggests that in 2002, 2.2 billion people −− more than a third of the world's population −− were potentially exposed to the malarial parasite. WHO uses a two−pronged approach for making its malaria estimates. For sub−Saharan Africa, where countries do not have an effective medical network for reporting cases of malaria, the agency uses "active" detection. In other words, doctors or health workers go to areas, try to establish how many people have fallen sick or died from malaria, and those figures are used to make an estimate for the whole country. For countries outside Africa, WHO uses the figures given to it by national governments.

Source: http://health.news.designerz.com/un−has−underestimated−malaria−cases−by−half−say−international−team.html?d20050309

18. *March 10, Honolulu Advertiser (HI)* — **Hawaii hit by late−season flu.** The number of flu cases reported in Hawaii soared during February, reaching nearly one in every 10 physician visits during the middle of the month −− and it may not yet have reached its peak. "I would probably still call it a moderate season, but we're not through yet. It's definitely late−peaking," said Sarah Park, deputy chief of the state Health Department's Disease Outbreak Control Division. The two major strains of flu hitting Hawaii residents this year do not appear to be particularly easier or harder on patients than those in other years, but they are hitting later than usual and it's not yet possible to say how serious the season will be. Nationwide, the number of flu cases began rising in December and have kept climbing. Influenza−like diseases have been reported in all 50 states. Park said that besides the normal December−to−March Northern Hemisphere flu season, Hawaii tends to have a persistent level of flu.
Source: http://the.honoluluadvertiser.com/article/2005/Mar/10/ln/ln1 0p.html

19. *March 09, Journal of the American Medical Association* — **Role of computerized physician entry systems in facilitating errors.** Hospital computerized physician order entry (CPOE) systems are widely regarded as the technical solution to medication ordering errors, the largest identified source of preventable hospital medical error. Published studies report that CPOE reduces medication errors up to 81 percent. Few researchers, however, have focused on the existence or types of medication errors facilitated by CPOE. Researchers performed a qualitative and quantitative study of house staff interaction with a CPOE system at a tertiary−care teaching hospital. They surveyed house staff; conducted five focus groups and 32 intensive one−on−one interviews with house staff, information technology leaders, pharmacy leaders, attending physicians, and nurses; shadowed house staff and nurses; and observed them using CPOE. Researchers found that a widely used CPOE system facilitated 22 types of medication error risks. Examples include fragmented CPOE displays that prevent a coherent view of patients' medications, pharmacy inventory displays mistaken for dosage guidelines, ignored antibiotic renewal notices placed on paper charts rather than in the CPOE system, separation of functions that facilitate double dosing and incompatible orders, and inflexible ordering formats generating wrong orders. Three quarters of the house staff reported observing each of these error risks, indicating that they occur weekly or more often.
Source: http://jama.ama−assn.org/cgi/content/full/293/10/1197

[Return to top]

Government Sector

20. *March 09, Government Executive* — **Homeland security technology grants.** The federal government could issue more than $11 billion in grants for homeland security technology over the next five years, according to a new report. The funding would provide money for state and local governments to implement technology projects in the areas of transportation, border and port security and personal identification, according to the report, which was produced by INPUT, a Reston, VA−based IT consulting firm. The money would pay for technologies created specifically for the purpose of border protection, seaport security and the safekeeping of mass transportation systems. "Anxiety over the safety of our major roadways and points of

entry has produced a large number of aggressive and valuable technology grant programs, covering many facets of transportation and border security," said Suzy Haleen, INPUT's manager of grant products and author of the report. Legislation introduced earlier this year by House lawmakers proposes $7.45 billion in spending for rail security over the next five years. The additional money would be allocated to technologies designed to prevent the capture of communications infrastructure. Railroad security spending would provide about $250 million in fiscal 2006 to upgrade freight railroads, the Alaska Railroad, hazardous materials shipping and Amtrak.
Source: http://www.govexec.com/dailyfed/0305/030905p1.htm

[Return to top]

Emergency Services Sector

21. *March 10, Sun and Weekly Herald (FL)* — **Search and rescue program helps firefighters.** As the walls crumbled and rain poured through the huge tears in the roof, a cadre of firefighters squeezed through window−size holes and combed meticulously through the debris to search for victims trapped in the damaged building. This was one of the real−life scenarios used during the Charlotte County Fire & EMS Special Operations Search and Rescue training program conducted Wednesday, March 9. The training was conducted inside the hurricane−ravaged Charlotte County Fire Station 7 in Punta Gorda, FL. The special operations unit worked for three days to practice their search and rescue skills in the event of another devastating hurricane or other disaster. The unit trained under the guidance of Safety Solutions, a state−contracted firefighter training organization comprised of firefighters from all over the country, said Deputy Chief of Special Operations Vern Riggall. Riggall said the county's preparedness is vital because after a disaster, the special ops units will be the first responder −− not FEMA or any other federal or state agency.
Source: http://www.sun−herald.com/NewsArchive2/031005/tp2ch6.htm?date=031005&story=tp2ch6.htm

22. *March 10, Government Technology* — **AMBER Alert 911 Web Portal wins industry achievement award.** The Washington State Department of Information Services (DIS) and the Washington State Patrol (WSP) were honored in the category of Outstanding Contribution to Digital Government during the Tenth Annual Washington Software Alliance Industry Achievement Awards banquet Tuesday, March 8. DIS and the WSP were recognized for their work on the AMBER Alert 911 Web Portal (http://www.amberalert911.com). The portal allows local law enforcement to simultaneously distribute real−time information about an abducted child to thousands of sources including other law enforcement organizations, the media, the public, transportation officials for electronic highway signs, lottery officials and many others. Through a simple sign−up process, thousands of people can receive information about an abduction via pagers, cell phones and e−mail accounts. This notification −− direct from law enforcement officials −− provides subscribers with the information needed to identify the suspect, thus helping law enforcement apprehend the suspect and save the child's life.
Source: http://www.govtech.net/news/news.php?id=93335

23. *March 09, Associated Press* — **Rutgers University professors develop software for large−scale evacuation plans.** Two Rutgers University professors are developing a computer

program to help large facilities develop procedures for evacuating people during a fire, bioterror attack or natural disaster. The software could be customized to fit any building plan. Once it detects anthrax or a fire, for example, it would provide security officials with specific steps to take, such as blocking off access to a contaminated area of a building. "It gives them directions and guidance on how to respond to the incident," said Ali Maher, professor and chairman of the civil and environmental engineering department at Rutgers in Trenton, NJ. The professors are testing their software now at Robert Wood Johnson University Hospital in New Brunswick, NJ. Rutgers is working with the Jet Propulsion Laboratory, managed by the California Institute of Technology in Pasadena, CA, and with a private firm to incorporate an anthrax detection technology in the program.
Source: http://www.nynewsday.com/news/local/wire/newjersey/ny−bc−nj−−terrorevacuations0309mar09,0,7317229.story?coll=ny−region−a pnewjersey

[Return to top]

Information Technology and Telecommunications Sector

24. *March 10, IDG News Service* — **World's most powerful computer is doubled in size.** Blue Gene/L, already ranked as the fastest supercomputer on the planet, has been doubled in size, according to researchers at Lawrence Livermore National Laboratory in Livermore, CA. Livermore has been running a 32,000−processor system since December, but three weeks ago trucks began delivering the components that allowed Livermore to add another 32,000 processors worth of power to the supercomputer, effectively doubling its processing power. Blue Gene/L is made up of approximately 32,000 two−processor nodes, giving it about 64,000 processors in total. A 33,000 processor prototype of Blue Gene/L, assembled by IBM last November was ranked the fastest computer on the planet on the Top500 list of the world's fastest supercomputers. IBM's prototype was benchmarked at 70.72 trillion calculations per second, or teraflops, using the Linpack benchmark, which puts the system through a series of mathematical calculations. Lawrence Livermore's new system is expected to be capable of approximately twice that performance, making it nearly three times as powerful as the next system on the list, NASA's 10,240−processor "Columbia" supercomputer. Columbia has been benchmarked at 51.87 teraflops.
Source: http://www.infoworld.com/article/05/03/10/HNcomputerdoublesi_1.html

25. *March 09, SecurityTracker* — **Novell iChain multiple vulnerabilities.** Multiple vulnerabilities were reported in Novell iChain GUI and Novell iChain Mini FTP Server. A remote user can gain administrative access, make unlimited login attempts without being locked out, or determine the installation path. Original advisories and updates available at:
http://support.novell.com/cgi−bin/search/searchtid.cgi?/1009 6885.htm and
http://support.novell.com/cgi−bin/search/searchtid.cgi?/1009 6886.htm and
http://support.novell.com/cgi−bin/search/searchtid.cgi?/1009 6887.htm
Source: http://www.securitytracker.com/archives/summary/9000.html

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: Multiple vulnerabilities have been reported in Novell iChain in the Mini FTP Server and GUI. For more information on these vulnerabilities, please visit the following link: http://www.securitytracker.com/

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