Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 09 June 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Columbian reports four train tankers derailed, spilling a flammable toxic chemical in a Vancouver rail yard and blocking the Burlington Northern Santa Fe Railway's main line between Vancouver and Seattle. (See item 10)
- Microsoft has released "Security Bulletin MS04−016: Vulnerability in DirectPlay Could Allow Denial of Service (Moderate)," and a patch is available on the Microsoft Website. (See item 32)
- Microsoft has released "Security Bulletin MS04−017 Vulnerability in Crystal Reports Web Viewer Could Allow Information Disclosure and Denial (Moderate)," and a patch is available on the Microsoft Website. (See item 33)
- US−CERT has released "Technical Cyber Security Alert TA04−160A: SQL Injection Vulnerabilities in Oracle E−Business Suite." (See item 34)

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: General; DHS/IAIP Web 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. *June 08, Associated Press* — **Natural gas prices expected to stay high.** While there is plenty of natural gas in storage, growing demand this summer will keep prices high, industry leaders predicted Tuesday, June 8. The Natural Gas Supply Association (NGSA) said it "expects

continuing upward pressure on prices this cooling season primarily due to projected warmer−than−normal weather, a strengthening economy and relatively flat production." According to Joseph Blount, the trade group's chairman, **one advantage this year is that the amount of natural gas in inventory is at about the five−year average, compared with a year ago, when inventories were dangerously low.** He said that according to a study commissioned by NGSA, **overall demand for natural gas will increase as much as three percent to 51 billion cubic feet a day this summer, with much of the increase as a result of demand by the electric power industry.** That, along with flat production will keep prices high, he said.
Source: http://www.nytimes.com/aponline/business/AP−Natural−Gas.html

2. *June 08, Reuters* — **Government sees gas pump prices easing in summer.** U.S. drivers should see slightly lower prices at the pumps later this summer when more oil exports from the Organization of Petroleum Exporting Countries (OPEC) arrive in U.S. ports, the federal government said Tuesday, June 8. The national price for regular unleaded gasoline will average $1.89 a gallon from July through September, down from the $1.94 previously estimated by the U.S. Energy Information Administration (EIA). Petroleum prices have started falling, with the national cost for U.S. gasoline down for a second straight week to $2.03 a gallon. **EIA, the Department of Energy's analytical arm, said "the declines are expected to continue" if there are no supply disruptions. "Potential price spikes are still quite possible given the uncertainties surrounding Middle East instability, terrorism, Iraq, and the fact that, while more optimism for improvement is warranted, oil inventories worldwide are still low," the agency said.** "In addition, currently low world oil surplus capacity levels provide an extremely limited cushion in the event of unexpected world oil market disruptions," EIA said.
Source: http://biz.yahoo.com/rb/040608/energy_eia_gasoline_1.html

3. *June 08, Baltimore Sun* — **Damage−control steps ordered in wake of Isabel. In the wake of widespread power outages last fall from Tropical Storm Isabel, the Maryland Public Service Commission (PSC) has ordered the state's utilities to take preventive steps aimed at reducing damage from storms and to improve communication with both emergency agencies and the public.** Isabel, one of the worst storms to strike the area in at least 50 years, left more than a million Marylanders without electricity in mid−September, some for more than a week. In the order issued Friday, June 4, the PSC told utilities to work on a plan to manage privately owned trees near power lines and to do a better job in educating the public about the hazards of planting trees close to utility rights−of way. It instructed them to work with local government and homeowner groups to selectively bury power lines to make service more reliable. The commission also ordered the state's utilities to improve coordination of storm restoration efforts with emergency agencies and asked utilities to give emergency management agencies written plans regarding programs for customers on life support equipment.
Source: http://www.baltimoresun.com/business/bal−bz.isabel08jun08,0,4204648.story?coll=bal−business−headlines

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

4. *June 07, Federal Computer Week* — **DoD plans Stinger tracker. Department of Defense (DoD) officials expect an electronic database and monitoring system for Stinger missiles to be in place later this year. Stingers are man−portable, shoulder−fired guided missile systems designed to shoot down low−altitude jets, propeller airplanes and helicopters.** The military is required to inventory every Stinger missile system sold overseas annually. DoD officials said a tool is being built now to have a database and monitoring system in place by October. The new system is meant to 1) give authorized users access to the data to determine the location or sale of Stingers and other weapons systems the department is required to monitor, 2) allow for the entry of serial numbers, notes, inspection histories and technical details on the weapons in the U.S. arsenal and those sold abroad, and 3) provide a method to track extract and report on all data.
   Source: http://www.fcw.com/fcw/articles/2004/0607/web−sting−06−07−04 .asp

[Return to top]

Banking and Finance Sector

5. *June 08, Finextra Research* — **Financial details for sale on online auction site. The current access codes and admin rights to the secure Intranet of one of Europe's largest financial services group was purchased on a hard drive over e−bay for just under USD$10 by UK security specialist Pointsec Mobile Technologies.** It was the first of 100 drives and laptops purchased as spare and used parts over Internet auction sites and other public auctions by the firm. **Pointsec found it was able to read seven out of 10 hard−drives bought in this way, all of which had supposedly been wiped−clean or re−formatted.** Pointsec also wanted to find out how easy it is to purchase and access information on laptops which are lost in transit such as at Gatwick or Heathrow airports or handed into the police. In all cases they found the laptops, and all the information residing on them, were put up for auction if they were not reclaimed after three months. Using password recovery software they were able to access the information on one in three of these laptops. This exercise was repeated in Sweden, the U.S. and Germany.
   Source: http://www.finextra.com/topstory.asp?id=11960

6. *June 08, Government Computer News* — **IRS, states expand efforts to fight money laundering.** The Internal Revenue Service (IRS) and state tax administrators are increasing information sharing to identify nonfilers, detect the abusive use of offshore payment cards and uncover money laundering. The IRS and states have uncovered tens of millions of dollars in previously unidentified abusive tax avoidance transactions, leading the federal and state tax agencies to expand their collaboration. **One of the new joint initiatives includes Title 31 Money Services Business Memorandum of Understanding. This agreement provides a framework for the federal−state exchange of compliance examination data associated with money services.** This initiative is the result of partnership efforts of the IRS, the Financial Crimes Enforcement Network and state regulatory agencies.

Source: http://gcn.com/vol1_no1/daily−updates/26149−1.html

7. *June 07, MSNBC* — **Consumers caught in credit card scam triangle.** A scam known as triangulation is on the rise again. "We're having a big problem out there right now −− this has happened to hundreds of people," U.S. Postal Inspector Barry Mew said. **Along with online retailer Amazon, the con artists seem to be targeting small, specialized e−commerce sites that sell tools and appliances. The scheme is so sophisticated that Julie Fergerson of the Merchant Risk Council, an Austin, TX−based consortium of companies that studies online fraud trends, suspects a single group or individual is behind the scam, which seems to come and go in spurts.** "This is a guess, but they may get between $50,000 and $500,000 in cash during a three to nine month period. Then, when we actually feel like law enforcement is getting close, he, or they, disappear," according to Fergerson. Mew said the recent spurt of activity has been going on for about six months. "The package is ordered as a gift so there's no billing information inside," he said. A glance at the packing slip won't reveal anything out of the ordinary. In fact, it's nearly impossible for consumers to spot the scam ahead of time.
Source: http://msnbc.msn.com/id/5158208/

8. *June 04, New Scientist* — **First quantum cryptography network unveiled.** The first computer network in which communication is secured with quantum cryptography is up and running in Cambridge, MA. **Quantum Net's (Qnet) creators say the implementation of more nodes in banks and credit card companies could make exchanging sensitive data over the internet more secure than it is with current cryptography systems.** The data in Qnet flows through ordinary fiber optic cables and stretches the 10 kilometers from BBN Technologies in Cambridge to Harvard University. It is encrypted using keys determined by the exchange of a series of single, polarized photons. Qnet is the first network consisting of more than two nodes to use quantum cryptography −− a more complex challenge. **Quantum cryptography guarantees secure communications by harnessing the quantum quirks of photons sent between users. Any attempt to intercept the photons will disturb their quantum state and raise the alarm.** At the moment computers capable of quantum cryptography are large and expensive, because they are custom−made. Chip Elliott, leader of the quantum engineering team, imagines a Qnet−like system may first appear in banks, for whom these factors might be less of a problem.
Source: http://www.newscientist.com/news/news.jsp?id=ns99995076

[Return to top]

Transportation Sector

9. *June 08, NBC News* — **Man stopped at Philadelphia International with almost $20,000 in cash.** A man was stopped over the weekend at the Philadelphia International Airport after security guards found what appeared to be a gun. Authorities said that nothing seemed right about the man who was trying to board a Northwest Airlines flight to Houston Saturday morning, June 5. His boarding pass stated that he was James Wood from New York City. But the Texas ID he produced said he was Yahkya Diarra from Houston. A New York driver's license he has showed again identified him as James Wood. At this point, police said, the man admitted that Wood was not his real name. **He identified himself as Yahkya Diarra. He was arrested for giving false ID and then officers were stunned when a search of his bag**

turned up $15,000 in $100 bills and Diarra also had another $4,700 on him in cash. The FBI and Homeland Security were contacted after Diarra told detectives that he is from Liberia and has lost his passport. With concerns over terrorism and money laundering, the Feds had a list of questions. Diarra originally said that the money wasn't his, and then claimed to be an art dealer and said the money was from the sale of art. Officials kept the money and released Diarra from custody.
Source: http://www.nbc10.com/news/3395089/detail.html

10. *June 08, The Columbian (WA)* — **Train cars derail, spill flammable chemical in Vancouver rail yard. Four train tankers filled with a flammable and toxic industrial chemical derailed in a Vancouver, Canada, rail yard on Monday afternoon, June 7, blocking the Burlington Northern Santa Fe Railway's main line between Vancouver and Seattle, WA.** No one was injured, but the accident forced firefighters and police to scramble to guard against an explosion and environmental contamination. Vancouver Fire Chief Don Bivins, who has worked in the city since 1985, said he could not recall a railway accident that was "potentially more dangerous." At 3:23 p.m. Monday, the tankers derailed for unknown reasons, leaving three on their sides and one upright. **Each tanker contained about 130 tons of styrene monomer, a liquid used to make polystyrene plastics, protective coatings and resins. Two of the tankers were leaking.** Firefighters and police quickly stopped all rail traffic, blocked streets and evacuated people from the rail yard near West 39th Street and Fourth Plain Boulevard. **Their biggest fear was an explosion, said Vancouver Fire Department spokesman Jim Flaherty. If the liquid reached 90 degrees, he said, it would begin to emit vapors that could ignite with a spark.** The cause was under investigation although sabotage has been ruled out.
Source: http://www.columbian.com/06082004/front_pa/153631.html

11. *June 08, NASA Press Release* — **NASA tests aviation turbulence detection system. A NASA developed technology that can automatically alert pilots of potentially dangerous turbulence will make its first evaluation flights on a commercial airliner. The idea behind NASA's Turbulence Prediction and Warning System (TPAWS) airborne radar is to give flight crews enough advance warning, so they can avoid turbulence or advise flight attendants and passengers to sit down and buckle up to avoid injury.** Researchers at NASA's Langley Research Center (LaRC), Hampton, VA, developed TPAWS to detect turbulence associated with thunderstorms as part of the NASA Aviation Safety and Security Program. Delta will install the TPAWS/Rockwell Collins radar unit on a Boeing 737−800 this summer. Delta flight crews will use and evaluate the technology during regularly scheduled flights in the U.S. and South America. The prototype is expected to fly for six to nine months. Researchers from NASA, the companies involved and the Federal Aviation Administration (FAA) will evaluate interim and final results of the turbulence prediction radar system. If the evaluation is successful, the technology may be adopted for new and existing aircraft.
Source: http://www.spaceref.com/news/viewpr.html?pid=14358

12. *June 08, Reuters* — **Boston police to search rail riders. Boston's transit police on Tuesday, June 8, announced plans to search subway and train riders to foil a possible a terror attack. Boston will be the first American city to employ random searches on public transport after March's deadly bombings in Spain, officials said.** "This is a proactive policy designed to deter and prevent a terrorist attack," Massachusetts Bay Transportation Authority

Police Chief Joseph Carter said. The random searches will begin in July, before July 4 Independence Day celebrations and ahead of the Democratic National Convention at the end of July. Work on transforming the site of the Convention from a sports arena to a political hall stopped on Tuesday however as construction workers walked away from the job, refusing to cross another union's picket line. Since early morning, hundreds of police, firefighters and emergency medical technicians have protested near the FleetCenter where the Convention will kick off on July 26. Tuesday's protests snarled traffic and sparked another round of criticism from locals already angry that train service to Boston's North Station will be halted during the Convention for security reasons.
Source: http://www.reuters.com/newsArticle.jhtml?type=topNews&storyI D=5375016

13. *June 08, USA TODAY* — **Fatal fire hazards find hiding places inside planes. The confusion and lack of effective training about how to deal with fires has shocked federal accident investigators, who say in interviews and public records that fires remain a serious threat to passenger aircraft. In a recent formal recommendation, the National Transportation Safety Board concluded that "training programs still do not adequately prepare crewmembers to fight the type of hidden in−flight fires likely to occur on airplanes."** Aviation regulators such as the Federal Aviation Administration have mandated many improvements in recent decades to protect flights from fires, and other actions are on the way. But regulators, airlines and aircraft manufacturers say that some of the proposals by safety advocates are impractical or could even make flights riskier, not safer. They say fatal fires already are extremely rare. **Accident investigators acknowledge that few planes have crashed because of fires: only three fatal accidents in the U.S. since 1980. But the number of unpublicized incidents, and the defenselessness of crewmembers against a raging fire, have convinced them that the risks are real.** The aviation industry has taken numerous steps in recent decades to reduce the risks from fires. But investigators in the U.S. and Canada say more needs to be done.
Source: http://www.usatoday.com/news/nation/2004−06−07−plane−fires_x .htm

14. *June 07, Associated Press* — **FAA proposes to fine two airlines $2.5M.** The Federal Aviation Administration (FAA) is proposing $2.5 million in civil penalties against Atlantic Coast Airlines and United Airlines for violating regulations. **Under the proposal Monday, June 7, the FAA alleges both airlines failed to follow required maintenance actions on specific aircraft and operated those planes when they weren't in compliance with regulations.** In the case of Atlantic Coast, now operating as Independence Air, the FAA proposes a $1.5 million penalty, saying the airline operated several of its aircraft without performing mandatory inspections of engines, airframes and other components. The agency said the airline failed to maintain its aircraft in according to Atlantic Coast's FAA−approved maintenance program. The FAA also claims Chantilly, VA−based Atlantic Coast did not have a properly functioning inspection program and did not keep appropriate maintenance records on its aircraft. The FAA proposed a $1 million penalty against United, based in Elk Grove Village, IL. The airline operated a Boeing 777 on about 263 flights in 2001 during which the escape slides would have been unusable during an emergency evacuation, the FAA said. An investigation found that safety maintenance pins installed in all eight of the plane's emergency escape slides caused the problem.
Source: http://www.chicagotribune.com/business/sns−ap−faa−airline−fi
nes,1,6994255.story?coll=chi−business−hed

15. *June 04, General Accounting Office* — **GAO−04−728: Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls (Report).** In the two years since passage of the Aviation and Transportation Security Act (ATSA), the Transportation Security Administration (TSA) has primarily focused its efforts on improving aviation security through enhanced passenger and baggage screening. The act also contained provisions directing TSA to take actions to improve the security of airport perimeters, access controls, and airport workers. The General Accounting Office (GAO) was asked to assess TSA's efforts to: (1) evaluate the security of airport perimeters and the controls that limit access into secured airport areas, (2) help airports implement and enhance perimeter security and access controls by providing them funding and technical guidance, and (3) implement measures to reduce the potential security risks posed by airport workers. **GAO is recommending that the Secretary of Homeland Security direct TSA's Administrator to develop and provide Congress with a plan for meeting the requirements of the Aviation and Transportation Security Act and taking other actions to improve airport security.** TSA reviewed a draft of this report and generally agreed with GAO's findings and recommendations. Technical comments were incorporated as appropriate. Highlights: http://www.gao.gov/highlights/d04728high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−728

[Return to top]

Postal and Shipping Sector

16. *June 08, Reuters* — **FedEx to get USPS international express business. The U.S. Postal Service (USPS) said on Tuesday, June 8, that FedEx Express, a unit of FedEx Corp., will on July 1 take over the delivery of its overseas Global Express Guaranteed packages from DHL Worldwide Express.** "About 7,400 Postal Service locations will offer the new co−branded service. As demand for this product grows, so will the number of Postal Service access points," the USPS said in a news release.
Source: http://www.reuters.com/newsArticle.jhtml?type=businessNews&s toryID=5371453

[Return to top]

Agriculture Sector

17. *June 08, Agence France Presse* — **New cattle disease found in Britain. British scientists have detected a previously unknown brain condition that caused paralysis and death in a young cow, officials said Tuesday, June 8.** The discovery is a new blow to an industry already badly hit by mad cow disease. An investigation had been launched after a white material was found on the brain of a heifer which died after suffering paralysis for around five or six days, Britain's Department for Environment and Rural Affairs said. The animals had been tested for known bovine diseases but none had been detected, a spokesman said. "The Veterinary Laboratories Agency (VLA) have recorded possibly a new condition in cattle in the United Kingdom," he said. **"In layman's terms, a type of cattle polio was identified which we haven't seen before."**

Source: http://www.thecouriermail.news.com.au/common/story_page/0,5936,9787656%255E1702,00.html

18. *June 07, Agriculture Online* — **Vesicular stomatitis in New Mexico horses. The National Veterinary Services Laboratories (NVSL) in Ames, Iowa Friday, June 4, confirmed the finding of vesicular stomatitis (VS) in horses on a farm in New Mexico.** On May 26, a foreign animal disease investigation was initiated at the Carlsbad, New Mexico farm, due to a report of tongue lesions in two horses on the premises. There are two additional horses, two steers and some sheep and goats on the infected premises that show no signs of lesions. Serum was taken from all horses on the premises and submitted to NVSL for testing. After the first round of testing, one horse was CF positive and three horses were cELISA positive for antibodies to the New Jersey strain of VS virus. The second set of serum samples from the horses were received by NVSL on June 3. Results from the second set of serum samples were consistent with the case definition for VS. **The infected premises has been placed under quarantine.**
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=sideBarMore__ANewsindex_html___51908

[Return to top]

Food Sector

19. *June 08, USAgNet* — **Russia bans EU meat imports. The European Commission (EC) has hit out at the decision of the Russian authorities to suspend imports from the European Union (EU) of food products of animal origin.** The Commission said it was surprised because discussions were ongoing on technical questions about veterinary certificates. "Any disruption of trade is unnecessary and unjustified. The measures put in place by the Russian authorities do not correspond to any scientific assessment of risk backed up by appropriate risk management measures," an EC spokesman said.
Source: http://www.usagnet.com/story−national.cfm?Id=605&yr=2004

20. *June 08, American Phytopathological Society* — **Fruit and vegetable safety.** Recent advances in food safety research are enabling plant pathologists to gain insight into how dangerous human pathogens, such as strains of E.coli and Salmonella, can survive on fresh fruits and vegetables and what can be done to control future outbreaks. According to Steve Scheuerell, faculty research associate at Oregon State University's Department of Botany and Plant Pathology, there has been an increase in reported human disease outbreaks associated with fresh produce over the last couple decades. "When an outbreak occurs, most of the infected produce has already been consumed," said Scheuerell. "Usually recalls won't help. This is why prevention is key to keeping food safe," he said. **To reduce the potential for the transfer of pathogens to fresh produce, plant pathologists are stressing the need to implement and maintain sanitary growing and harvesting conditions worldwide. "As the U.S. increases its importation of produce, it is increasingly important to us that growers everywhere have good quality irrigation water and sanitary conditions for their workers,"** Scheuerell said. "Using techniques developed by plant pathologists, scientists are just beginning to understand how human pathogens colonize leaf surfaces, and how their survival can be influenced by manipulating leaf surface microflora and environmental conditions," he said.

Source: http://www.eurekalert.org/pub_releases/2004−06/aps−kyp060804 .php

21. *June 08, Agence France Presse* — **Nigerian government to destroy packs of noodles. The Nigerian food safety agency is to destroy 764,444 packs of noodles withdrawn from circulation following investigations that they could be dangerous.** Indian−owned De−United Foods Limited, makers of Indomie brand noodles, said in a statement Tuesday, June 8, that following an order by the state−run food and drugs agency NAFDAC, it has withdrawn the suspected packs from the market. "A total of 764,440 packs have been transferred to NAFDAC custody for destruction," it said. At least one person was believed to have died in May while others fell ill after eating the noodles, officials said. NAFDAC officials shut down for a week the Ota and Port Harcourt factories of the company. The factories were reopened of May 20 after the agency's investigation. Indomie instant noodles are a favourite among urban Nigerian children.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=5&u=/afp/20040608/hl_afp/nigeria_health_food_0406081558 20

[Return to top]

Water Sector

22. *June 08, Water Tech Online* — **Cincinnati may play key role in fight against water terrorism. Cincinnati, OH, which already hosts a center devoted to research on preventing and responding to water terrorism and other acts of terror, will be a pilot city for a program designed to help cities respond better to chemical or biological attacks, according to an article by the Cincinnati Enquirer.** A representative from the U.S. Department of Homeland Security, along with Senator George Voinovich, made the announcement Monday, June 7, at a 40,000 square−foot facility that will be the high−tech base of the research project. Three other cities will be selected for the $10 million pilot program. Cincinnati was chosen because it already houses a federal research center that is focused on preventing water terrorism and the cleaning up of contaminated buildings in the event of a chemical or biological attack.
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=48250

23. *June 08, University of California − Irvine* — **Perchlorate may be acceptable in drinking water at higher levels. Even at significantly higher levels than recommended by California's leading health assessment agency, the contaminant perchlorate in drinking water seems to pose no additional risks to healthy people, according to a recent report issued by the University of California − Irvine Urban Water Research Center.** Produced by an independent committee of scholars, the center's report is being provided to the California Department of Health Services and other policymakers as they wrestle with setting a statewide standard for perchlorate in drinking water. The committee viewed the Office of Environmental Health Hazard Assessment's current public health goal of six parts per billion (ppb) as well reasoned and in keeping with a value set only on health considerations. Its findings, however, show that exposure to perchlorate at levels below 100 parts per billion would still protect the public health. **Perchlorate has been found throughout California in approximately 350 wells in 89 water systems; 90 percent of these are located in Southern California. Los Angeles, Orange, San Bernadino and Riverside counties report 40 to 89 percent of the**

water systems tested contain perchlorate levels greater than six ppb. A copy of the report is available at http://www.urban−water.uci.edu/index.asp.
Source: http://www.eurekalert.org/pub_releases/2004−06/uoc−−ucf06080 4.php

24. *June 05, Chicago Tribune* — **Equipment quickly detects bacteria in lake water. Starting next week, new equipment anchored to the bottom of Lake Michigan will more quickly detect potentially harmful levels of bacteria at two Lake County beaches, officials said Friday, June 4.** Instead of waiting 24 hours for the information needed to impose a swimming ban, Lake County, IL, Health Department officials will know within three hours whether there are high E. coli levels in the water at Lake Forest Beach and South Beach at Illinois Beach State Park. Last year, 178 beach closings were reported in Lake County. The new equipment is being drilled into the bottom of Lake Michigan, hundreds of feet from shore. **It will monitor rainfall, air temperature, water clarity, wind direction and speed, and relative humidity, which can predict E.coli contamination.** The equipment will send information via radio waves to a land−based computer system.
Source: http://www.chicagotribune.com/news/local/west/chi−0406050116 jun05,1,4332157.story?coll=chi−newslocalwest−hed

[Return to top]

Public Health Sector

25. *June 08, Oakland Tribune* — **U.S. bioterrorism research. The Bush administration is ramping up bioterrorism research that will press beyond traditional defenses against natural biowarfare germs to explore genetically engineered superbugs, as well as the means to mass−produce and disseminate them.** Defense scientists say broader studies of bioterror threats are needed to weigh the chances of certain attacks, tell U.S. intelligence what to look for, and shore up defenses. "Mother Nature has created a number of nasty pathogens. But we have to be worried about the future, too, and worry about comprehensive threats," said Gerald Parker, head of science−based threat analysis and response for the U.S. Department of Homeland Security. **The rapid spread and dropping costs of basic biotechnology raise the specter that terrorists eventually will tinker with naturally deadly germs to make them more virulent, impervious to drugs, or more difficult to detect.**
Source: http://www.oaklandtribune.com/Stories/0,1413,82~1865~2199592 ,00.html

26. *June 08, Associated Press* — **Officials seize ephedra packets. Federal officials have seized more than 3,000 packets of the banned supplement ephedra, from a warehouse, bound to hundreds of convenience stores in Florida.** The raid in late May was part of a series of spot checks state food inspectors have started making since the product was banned nearly two months ago. Officials have found about 6,700 packets of ephedra at 182 locations, according to the Florida Department of Agriculture and Consumer Services. The U.S. Food and Drug Administration banned the sale of ephedra products as of April 12, linking it to 155 deaths. Though ephedra is now off the shelves of most health−food chain stores, it can still be found in some gas stations and convenience stores, which are more difficult to police.
Source: http://msnbc.msn.com/id/5163714/

27. *June 04, Genome News Network* — **Deaths blamed on microbe with anthrax genes. Last year two hospital patients from different cities in Texas died of severe pneumonia that appeared to be caused by inhalation anthrax.** Yet neither patient was infected with the bacterium that causes anthrax, Bacillus anthracis. **Instead, DNA tests indicated that both patients became infected by another species of bacteria that carried the lethal anthrax genes.** The bacterium, called Bacillus cereus, typically causes mild food poisoning. When the Texas cases came to light, researchers at the U.S. Centers for Disease Control and Prevention (CDC) were sequencing the genome of a strain of B. cereus isolated from a man in Louisiana who, in 1994, developed severe anthrax−like symptoms. **The researchers now report that B. cereus can indeed carry lethal genes of the anthrax bacterium.** The Texas and Louisiana patients were all metal workers and appeared to have inhaled the bacteria, although scientists do not know how. **These are the first cases in which anthrax genes have been discovered in an organism other than B. anthracis, and the findings raise concerns about the prevalence of the previously unknown pathogen and our preparedness to detect and respond to it in the event of a biological attack.** For example, tests used to detect anthrax during a suspected bioterrorism incident might not pick up the equally pathogenic bacteria B. cereus.
Source: http://www.genomenewsnetwork.org/articles/2004/06/04/anthrax_genes.php

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

28. *June 08, Southwest Sun (Sugarland, TX)* — **Texas area gets $1 million for security.** With more than $1 million of Homeland Security Grants going to Fort Bend County and area cities, county and city officials plan to improve the coordination of operation among the 13−counties that make up the Houston−Galveston Area Council. Fort Bend County's Director of Emergency Management Jeff Braun says that after the terrorist attacks on September 11, 2001, the federal government began to assist local governments in bolstering equipment and training to help prevent terrorism acts. Several funding programs were designed to combat terrorism, but the most recognized is the State Homeland Security program, which Braun said has been around since 2002. **Also, new this year is a separate grant earmarked for law enforcement terrorism prevention, Braun said. Braun said this year the federal government used a formula based on an area's population and potential threats to determine how much it would receive. Only cities with a population over 25,000 received a base grant, he said.** The majority of the funding will go to Houston and Harris County, which have the most threat elements.
Source: http://www.zwire.com/site/news.cfm?newsid=11896457&BRD=1914&PAG=461&dept_id=183407&rfi=6

29. *June 08, Associated Press* — **Fire Department increases Hazmat training.** The New York City Fire Department announced Tuesday, June 8, that 70 members of its new new hazardous

materials (Hazmat) technician units have received specialized training. The Hazmat technician units, consisting of 25 to 30 firefighters, are based at three existing companies: Engine Company 44 on the Upper East Side, Engine Company 274 in Astoria, Queens, and Engine Company 165 on Staten Island. The 80−hour advanced training course "further demonstrates the commitment the Fire Department has to providing the people of New York with the best protection against the new threats we now face," said Fire Commissioner Nicholas Scoppetta. **"They will also enhance and decentralize the department's response to multiple incidents involving hazardous materials and life safety operations." Since September 11, 2001, the Fire Department has trained more than 700 members in advanced hazardous materials operations, increasing their numbers from 430 to more than 1,100.**
Source: http://www.nynewsday.com/news/local/manhattan/ny−bc−ny−−hazmatcapabilitie0608jun08,0,6610144.story?coll=nyc−moreny−headl ines

30. *June 07, Department of Homeland Security* — **Homeland Security launches Regional Technology Integration. The Department of Homeland Security, on June 7, announced a new initiative called Regional Technology Integration (RTI) in Cincinnati, OH, to facilitate the transition of innovative technologies and organizational concepts to regional, state, and local jurisdictions.** Through the program, managed by Homeland Security's Science & Technology directorate, four urban areas across the country have been selected to be the initial pilot locations for this program. The Cincinnati urban area is one of these four. All of the selected regions are currently participating in the Homeland Security Urban Area Security Initiative and have demonstrated a willingness and capacity to adopt advanced and innovative concepts for emergency preparedness and public safety. For further information refer to http://www.dhs.gov/dhspublic/display?content=3704.
Source: http://www.dhs.gov/dhspublic/display?content=3707

[Return to top]

Information Technology and Telecommunications Sector

31. *June 08, CNET News.com* — **AT&T plans Net phone trials in Asia, Europe.** AT&T is taking its Internet telephony services to enterprises in Asia and Europe. **On Tuesday, June 8, the company announced plans to conduct trials of its voice over Internet Protocol (VoIP) service in Australia, Hong Kong, Singapore and the UK. The trials are slated to start in the third quarter and will be targeted to multinational companies.** AT&T expects to launch the service in 2005. The offerings for Asian and European markets are based on the company's CallVantage service, which launched in the United States in March and was expanded last month. CallVantage is designed to enable workers to use VoIP from their homes or hotels over available broadband connections.
Source: http://news.com.com/AT%26%2338%3BT+plans+Net+phone+trials+in+Asia%2C+Europe/2100−7352_3−5228515.html?tag=nefd.top

32. *June 08, Microsoft* — **Microsoft Security Bulletin MS04−016: Vulnerability in DirectPlay Could Allow Denial of Service. A denial of service vulnerability exists in the implementation of the IDirectPlay4 application programming interface (API) of Microsoft DirectPlay because of a lack of robust packet validation**. If a user is running a networked DirectPlay application, an attacker who successfully exploited this vulnerability could cause the

DirectPlay application to fail. The user would have to restart the application to resume functionality. Microsoft recommends that customers should consider applying the security update. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that customers consider applying the security update.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−016. mspx

33. *June 08, Microsoft* — **Microsoft Security Bulletin MS04−017 Vulnerability in Crystal Reports Web Viewer Could Allow Information Disclosure and Denial of Service.** Microsoft Visual Studio .NET 2003 (all versions) and Outlook 2003 with Business Contact Manager redistribute Crystal Reports and are therefore affected by the vulnerability. Microsoft Business Solutions CRM 1.2 redistributes Crystal Enterprise, which is affected in the same way. **An attacker who successfully exploited the vulnerability could retrieve and delete files through the Crystal Reports and Crystal Enterprise Web viewers on an affected system**. The number of files of files that are impacted by this vulnerability would depend on the security context of the affected component that is used by the Crystal Web viewer. Systems can only be vulnerable if they have Internet Information Services (IIS) installed. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that customers consider applying the security update.
Source: http://www.microsoft.com/technet/security/bulletin/MS04−017. mspx

34. *June 08, US−CERT* — **Technical Cyber Security Alert TA04−160A: SQL Injection Vulnerabilities in Oracle E−Business Suite.** Oracle E−Business Suite is a set of applications and modules that enables an organization to manage customer interactions, deliver services, manufacture products, ship orders, collect payments, and other tasks using a single database model. According to the Oracle Security Alert 67, **Oracle Applications 11.0 (all releases) and Oracle E−Business Suite Release 11i, 11.5.1 through 11.5.8 are vulnerable to SQL injection vulnerabilities**. Oracle E−Business Suite Release 11.5.9 and later are not vulnerable. This vulnerability is not platform specific. Note that no authentication mechanisms of Oracle E−Business Suite will mitigate exploitation of the attack. Patches and related information are available from: http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=274375.1
Source: http://www.us−cert.gov/cas/techalerts/TA04−160A.html

35. *June 07, CNET News.com* — **Apple patches 'critical' OS X flaw.** Apple Computer on Monday, June 7, released a security patch that fixes what the company called the first "critical" Mac OS X flaw. **A combination of holes disclosed by security researchers last month could have allowed an attacker to take over a vulnerable Macintosh, though no such exploits have been reported**. Apple issued a partial fix last month, but security researchers had said that the Mac remained open to attack. The patch, which was made available via Mac OS X's Software Update, attempts to prevent such problems by warning users when a program is being launched via the Internet that has not previously been run on the system. Apple also took other steps in Mac OS X and the Safari Web browser to try to keep unintended applications or files from being opened. Apple said the update is being made available for those running version 10.3.4 of Mac OS X Panther and version 10.2.8 of Mac OS X Jaguar, as well as the corresponding server versions. **Apple is still investigating whether the flaw exists in earlier versions of the Mac OS.**
Source: http://news.com.com/Apple+patches+%27critical%27+OS+X+flaw/2

100−7355_3−5228038.html?tag=nefd.top

36. *June 07, US−CERT* — **Vulnerability Note VU#961579: Oracle E−Business Suite SQL Injection vulnerabilities.** According to the Oracle Security Alert 67, Oracle Applications 11.0 (all releases) and Oracle E−Business Suite Release 11i, 11.5.1 through 11.5.8 are vulnerable to SQL injection vulnerabilities. This vulnerability is not platform specific. **An unauthenticated attacker may be able to exploit this vulnerability to execute procedures or SQL queries and updates inside the database**. This may lead to compromise of the system and data integrity issues. Patches and related information are available from: http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=274375.1
Source: http://www.kb.cert.org/vuls/id/961579

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.

Watch Synopsis: There is a new Worm called Plexus that exhibits many of the same characteristics that MyDoom exhibited. The initial variant does not target federal or military systems, but we can be certain that future variants may do so. This worm appears to be a blended threat and propagates by at least 5 various methods.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 1026 (nterm), 1027 (icq), 1434 (ms−sql−m), 137 (netbios−ns), 445 (microsoft−ds), 9898 (dabber), 5554 (sasser−ftp), 3127 (mydoom), 139 (netbios−ssn) 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]

General Sector

37. *June 08, Reuters* — **Italy arrests suspected Madrid bombing mastermind.** Italy arrested an Egyptian man suspected of helping to plan the Madrid train bombings as police across Europe swooped on Islamic militants in coordinated anti−terror raids, officials said Tuesday, June 8. **Rabei Osman Sayed Ahmed, known as "Mohamed the Egyptian," was seized in Milan in a operation that Italian Interior Minister Giuseppe Pisanu said was aimed at a "dangerous group of terrorists close to al Qaeda" which had been planning more attacks.** Ahmed was one of at least 17 people arrested in coordinated operations in Italy, France, Belgium, and Spain. "He is considered one of the masterminds of March 11," a Spanish Interior

Ministry spokesman said, referring to the attacks that killed 191 people in the Spanish capital. Pisanu said the man was one of the "principal executors" of the Madrid bombings. Fifteen of the arrests came in Belgium, and those held there included Jordanians, Palestinians, Egyptians, and Moroccans. "We know them to be part of a terrorist group," said Glenn Audenaert, director of the federal police bureau of Brussels.
Source: http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=5373215

38. *June 08, Washington Post* — **Cigarette smuggling linked to terrorism. Smugglers with ties to terrorist groups are acquiring millions of dollars from illegal cigarette sales and funneling the cash to organizations such as al Qaeda and Hezbollah,** federal law enforcement officials say, prompting a nationwide crackdown on black market tobacco. The federal Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) has more than 300 open cases of illicit cigarette trafficking −− including several with terrorist links −− up from only a handful five years ago, ATF sources said. The lucrative trafficking of cigarettes, known as cigarette diversion, is a simple scheme but difficult to stop, law enforcement officials say. The traffickers purchase a large volume of cigarettes in states where the tax is low, and then sell them at a discount. **With huge profits −− and low penalties for arrest and conviction −− illicit cigarette trafficking now has begun to rival drug trafficking as a funding choice for terrorist groups,** said William Billingslea, an ATF senior intelligence analyst who has studied the issue extensively. Although black market cigarette sales have been around for decades, the link to suspected terrorist groups is a new and growing phenomenon.
Source: http://www.washingtonpost.com/wp−dyn/articles/A23384−2004Jun7.html

[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. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − 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.

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.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

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 an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.