Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 23 June 2004

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports New York City building superintendents and doormen are receiving anti−terrorism training under a program developed with the help of the Police Department. (See item 26)
- US−CERT has released Technical Cyber Security Alert TA04−174A: Multiple Vulnerabilities in ISC DHCP 3. (See item 31)
- Techworld reports that according to security firm eEye, hackers could use two IBM ActiveX controls designed for automated PC support to attack PCs through the Internet Explorer browser. (See item 32)

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 22, The News−Item (PA)* — **Fire at co−generation plant. More than 100 firefighters battled a fire Saturday, June 19, at the Gilberton Power Station co−generation plant in Gilberton, PA. The fire at the John B. Rich Memorial Power Station was discovered at about 4 p.m. in a building that houses the turbines and boilers used in the co−generation process,** said James Hampford of the Schuylkill County Emergency Management Agency. Fire officials said thick pads of insulation between a roof and an inner roof caught fire and were smoldering. Firefighters had difficulty reaching the flames from the inside due to a heavy metal

barrier below the insulation. Also, getting at the blaze from above proved just as hard since the plant's roof is covered by stone. The building, said to be more than seven stories tall, also made the firefighting task difficult because of the exertion it took to reach the roof. The power plant never stopped operating. Officials said a fire marshal will investigate the cause of the fire. Source: http://www.zwire.com/site/news.cfm?newsid=12045429&BRD=2311&PAG=461&dept_id=482260&rfi=6

2. *June 22, Reuters* — **Panel to examine refining capacity, oil stocks. A federal advisory panel will assess U.S. oil refining capacity and crude oil stocks to see if steps can be taken to boost energy supplies, U.S. Secretary of Energy Spencer Abraham said** on Tuesday, June 22. "There is no question that one of the significant energy challenges we face is insufficient refinery capacity," Abraham said at a meeting of the National Petroleum Council. The council, made up of oil and natural gas industry executives, is a federal advisory committee to the U.S. energy secretary. Abraham also asked the council to study current assumptions about adequate U.S. crude oil inventories. **The industry now uses a threshold of 270 million barrels to determine whether supplies are adequate or not, but Abraham questioned whether that assumption is "still appropriate."** The crude inventory threshold has been a moving target for an industry that has seen many drilling advances over the last few decades. Record−high retail gasoline prices last month prompted some Republican lawmakers to urge construction of the first new U.S. oil refinery in three decades. Experts estimate building a new refinery would cost upwards of $1 billion. The last independent U.S. refinery was built in 1976. Source: http://www.reuters.com/newsArticle.jhtml?type=politicsNews&s toryID=5484235

3. *June 22, General Accounting Office* — **GAO−04−894T: Nuclear Security: Several Issues Could Impede the Ability of DOE's Office of Energy, Science and Environment to Meet the May 2003 Design Basis Threat (Testimony). A successful terrorist attack on Department of Energy (DOE) sites containing the material used in nuclear weapons, called special nuclear material, could have devastating consequences for the site and its surrounding communities. Because of these risks, DOE needs an effective safeguards and security program.** A key component of an effective program is the design basis threat (DBT), a classified document that identifies, among other things, the potential size and capabilities of terrorist forces. The terrorist attacks of September 11, 2001, rendered the then−current DBT obsolete resulting in DOE issuing a new version in May 2003. The General Accounting Office (GAO) examined the issues that could impede the ability of DOE's Office of Energy, Science and Environment to fully meet the threat contained in the May 2003 DBT by the department's fiscal year 2006 deadline. Highlights: http://www.gao.gov/highlights/d04894thigh.pdf Source: http://www.gao.gov/new.items/d04894t.pdf

4. *June 22, Reuters* — **U.S. gas prices fall again. The average U.S. retail gasoline price has dropped for the fourth consecutive week, falling to 4.8 cents a gallon to $1.937, the federal government said Monday, June 21. However, average pump prices are still 44 cents a gallon higher than a year ago, according to the Energy Information Administration (EIA),** the U.S. Department of Energy's analytical arm. The fall reflects declining crude oil prices, which account for almost half the cost of making gasoline. The Organization of Petroleum Exporting Countries promised to send more oil tankers to the U.S. market to replenish supplies and lower petroleum prices. The EIA's weekly gasoline report also found the retail price for cleaner−burning reformulated gasoline, sold in polluted metropolitan areas, dropped 3.8 cents

to $2.072 a gallon. Separately, the EIA survey said the average pump price for diesel fuel dropped 1.1 cents to $1.70 a gallon, but remained about 28 cents higher than a year ago.
Source: http://msnbc.msn.com/id/5267885/

5. *June 22, Reuters* — **Oil prices up after refinery glitch. Oil prices rose on Tuesday, June 22, after the shutdown of a gasoline−making unit at a key Texas refinery threatened to tighten supplies in the early days of the U.S. summer driving season.** The fuel production glitch added to concerns over stalled Iraqi oil exports after sabotage attacks last week and a Norwegian oil workers' strike. The news of an outage at the ConocoPhillips refinery in Lake Charles, LA, overcame bearish concerns that U.S. petroleum supply will show a rise when the U.S. government issues weekly data Wednesday, June 23. Tuesday, sources said **the Lake Charles plant was forced to delay the restart of a shut gasoline−making unit that has taken gasoline out of the strained U.S. supply chain. There was no immediate word when the plant would return to service,** which re−ignited concerns over gasoline supplies during the summer U.S. driving season.
Source: http://www.washingtonpost.com/wp−dyn/articles/A60868−2004Jun 22.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *June 22, Penn Live* — **Tanker explosion, chemical leak closes Erie freeway.** A tanker truck exploded Monday night, June 21, spilling chemicals on a freeway and injuring one person. Emergency crews on Tuesday were trying to clear wreckage from Interstate 90. **State police said a corrosive chemical mixture of sodium hydrochlorite and sodium hydroxite was mistakenly placed into the truck's aluminum tank. The mixture should have been transported in a stainless steel tank.** State police had stopped the truck around 8 p.m. because it was leaking its load onto Interstate 90 near the Interstate 79 interchange. The truck exploded about 30 minutes later, injuring one bystander. Emergency crews were trying to contain the chemical, which leaked into the highway drainage system. Crews worried that heavy rain showers forecast for Tuesday morning would spread the contamination. Westbound lanes on I−90 were open Tuesday morning, though only one lane was open for eastbound motorists.
Source: http://pennlive.com/newsflash/pa/index.ssf?/base/news−17/108 7907353164630.xml

[Return to top]

Defense Industrial Base Sector

7. *June 22, Government Computer News* — **Common weapon platform needed.** The Department of Defense's transformation initiative has "built up a bow wave of change," Air Force Maj. Gen. Marc Rogers said on Tuesday, June 22, at a conference. However, **military restructuring and user training must advance far more rapidly, until "any certified controller from any service can control any weapon platform," Rogers said. "We need a common, deployable, standardized command−and−control facility to work in and train for, just like we use a workstation in ordinary jobs," he said.** It might look like a workstation, Rogers said, "but it's called a weapon station, and it will have hundreds of

switches. There's no time for hunt and peck" searching for the right tool at a weapon station, so "it's all about training" of the decision−makers as well as the shooters. Besides a common weapon station, the military services must have interoperable data, he said.
Source: http://www.gcn.com/vol1_no1/daily−updates/26323−1.html

[Return to top]

Banking and Finance Sector

8. *June 18, Department of Treasury* — **Treasury to extend the "make available" provisions.** The Department of Treasury on Friday, June 18, announced its decision to extend the "make available" provisions of the Terrorism Risk Insurance Act (TRIA) through 2005, the third year of the federal Terrorism Risk Insurance Program. **The "make available" provisions of TRIA require that, from the date of enactment (November 26, 2002) through the last day of the second year of the Program (December 31, 2004), each insurer must make available, in all of its commercial property and casualty insurance policies, coverage for losses due to covered acts of terrorism that does not differ materially from the terms, amounts and other coverage limitations applicable to losses arising from events other than acts of terrorism.** TRIA requires that the Secretary of the Treasury determine whether the "make available" provision should be extended through the third and final year of the Program by September 1, 2004. Although Treasury had until September 1, 2004 to determine whether or not to extend the "make available" provisions of TRIA, the determination was made well in advance of the deadline in order to avoid any potential disruption in the terrorism risk insurance market.
Source: http://www.treasury.gov/press/releases/js1734.htm

[Return to top]

Transportation Sector

9. *June 22, Department of Transportation* — **DOT investment for Louisville means airport can take advantage of growing cargo trend. Thanks to a new $6.2 million grant announced on June 22 by the U.S. Department of Transportation (DOT), the Louisville International Airport will be ready to take advantage of rapid growth in air freight,** a senior U.S. transportation official said. The grant will fund an extension of the airport's main cargo runway to allow fully loaded cargo flights from Louisville direct, non−stop flights as far away as China, he said. In addition, the grant is funding work to realign sections of Martha Maloney Boulevard to make it easier for cargo trucks to bring goods into and out of the airport, easing traffic near the airport, Duvall added. The grant announcement came as the Department simultaneously released a new national survey of the cargo industry titled Freight Shipments in America. The study found that air freight, including the shipment by air−truck combinations, was the fastest growing method of freight shipment over the past decade, with the total value of air freight virtually doubling from 1993 to 2002 to $2.7 billion a day.
Source: http://www.dot.gov/affairs/dot09204.htm

10.

June 22, The Trucker — **'If it doesn't look right,' Highway Watch wants to hear about it.** "When it just doesn't look right, we want to hear from you," security specialist Jeff Beatty told some 65 truckers, bus drivers and other transportation workers June 18 at North Little Rock, AR. The Arkansas workers underwent nearly two hours of training to learn how to spot potential terrorist activity on the nation's highway infrastructure. **By March 2005, it's hoped there will be an estimated 400,000 transportation employees nationwide who have been trained to be the country's "eyes and ears" in spotting terrorist activity.** Highway Watch is being administered by the American Trucking Association under a cooperative agreement with the Transportation Security Administration. **High on the list of what to watch for was making sure a truck or other vehicle isn't used as a weapon.** "Think fuel, think incendiary device, think explosives," Beatty said. Specifically, transportation workers were asked to be on the lookout for parked, occupied vehicles; anyone asking a lot of questions −− especially concerning routes or loads or drop−off times; someone taking photographs; or any out−of−place or suspicious activity.
Source: http://www.thetrucker.com/stories/06_04/0622_watch_program.h tml

11. *June 22, Computerworld* — **Logan Airport using BlackBerries for background checks.** Long a popular gadget for lawyers and businessmen, the BlackBerry wireless handheld device has now been drafted into the U.S. war on terrorism. **Massachusetts State Police officers patrolling Boston's Logan International Airport are using BlackBerries to perform background checks on suspicious individuals.** State police checking up on suspicious persons and vehicles in the field can compare information at the scene to an Internet−based XML database, which contains information on more than 200 million U.S. residents, according to a statement attributed to Massachusetts State Police Lt. Thomas Coffey. The database integrates data from a wide variety of public and private sources, such as motor vehicle records. **Among other things, the database service has features that let authorities perform reverse lookups on some cellular telephone numbers and unlisted numbers.**
Source: http://www.computerworld.com/governmenttopics/government/itg overnment/story/0,10801,94025,00.html

12. *June 22, Associated Press* — **Metro chief tells lawmakers more money needed for security. The top man at Metro, in Washington, DC, says the transit agency needs a lot more money to make sure the system is safe from terrorists.** Richard White is telling a House subcommittee that there's a long list of high priority security needs. In prepared testimony, the Metro CEO says that includes enhancing their ability to detect weapons of mass destruction. **White says Metro also should have more video cameras on its buses, better PA systems in subway stations, and more anti−terror equipment for the transit police.** White says in the last two years, the Department of Homeland Security has spent more than $9 billion dollars on aviation security −− but just $115 million on transit security. He says **unlike with planes, when it comes to mass transit you have to focus not only on deterrence but also on mitigating the impact of a potential attack.**
Source: http://www.wtopnews.com/index.php?nid=25&sid=215636

13. *June 21, MSNBC* — **Port plugs in ships to cut diesel pollution.** Environmental groups claimed a victory Monday, June 21, when the Port of Los Angeles adopted for container ships a technology that's long been used by other watercraft: plugging them into the power grid while docked instead of running dirty diesel engines. **The new terminal fulfills part of a legal**

settlement by the Port of Los Angeles, which had been sued by activists who argued that the terminal was being built without proper studies on the health effects on local neighborhoods. The Coalition for Clean Air, a plaintiff in the lawsuit, called it a win−win solution. "These ports are America's gateway to Asia, which means they'll be growing rapidly for a long time to come," said Todd Campbell, the group's policy director. "However, growth cannot come at the expense of our environment and public health. Today we're unveiling a tool that will help us keep pollution in check without stifling economic expansion." The activists include the Natural Resources Defense Council, which noted that the ports of Los Angeles and nearby Long Beach are the single largest source of air pollution in Southern California — emitting as much diesel exhaust as 16,000 tractor−trailers idling their engines 24 hours a day. The new terminal is expected to eliminate more than three tons of nitrogen oxides and 350 pounds of diesel particulate matter for each ship that plugs in.
Source: http://msnbc.msn.com/id/5263065/

14. *June 17, Transportation Security Administration* — **TSA pledges $15 million to San Francisco International.** Rear Adm. David M. Stone, USN (Ret.), Acting Administrator for the Transportation Security Administration (TSA), on June 17, announced TSA has signed a contract with the Airport Commission for the City and County of San Francisco for $15 million **to offset the costs of completing a permanent in−line Explosives Detection System (EDS) at San Francisco International Airport.** The contract is part of TSA's commitment to achieving maximum security, efficiency and passenger convenience through a permanent in−line EDS−based screening system. "TSA continues to work with the airport commission to meet growing demand and maintain the highest security standards for San Francisco International Airport," said Admiral Stone. "This work will lead to more efficient baggage screening – serving security and improving customer service." The Project will require the Commission to perform the entire scope of work associated with not only the installation of integrated and non−integrated EDS equipment, but also the improvements to be made to the existing screening configurations in the baggage handling system at SFO.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 00b0ccd

[Return to top]

Postal and Shipping Sector

15. *June 22, DM News* — **Postal Service income over budget. The U.S. Postal Service had net income of $2.9 billion −− $918.9 million over budget −− from October 1 to May 31, the agency reported Monday, June 21.** Meanwhile, mail volume was up and expenses are under plan. According to the Postal Service's fiscal and operating statements, revenue was $46.65 billion, 0.5 percent better than planned, while expenses of $43.75 billion were 1.5 percent under the planned budget. Mail volume rose 0.7 percent compared with last year. Standard mail and International mail grew 3.8 percent and 6.9 percent, respectively. However, several mail classes saw declines. Periodicals fell 4.4 percent; Express Mail, 4.2 percent; Priority Mail, 2.4 percent; First−Class, 1.7 percent; and Package Services, 0.2 percent.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2873 1

16. *June 22, Datamonitor* — **Cargo carriers benefit from U.S.−China accord.** The bilateral accord signed by China and the U.S. last week will more than double the number of U.S.

airlines that can operate to and from the People's Republic, and will permit an extra 111 weekly flights by all−cargo carriers. UPS, FedEx and American Airlines have welcomed the agreement, which will dramatically increase air cargo volumes between the two countries. The volume of trade in goods between the U.S. and China has risen dramatically in recent years, to the point where the U.S. is China's second−largest trading partner. **To facilitate continuing increases in trade, the two countries have signed an air services agreement that will allow air cargo capacity to keep up with growing demand. Integrators FedEx and UPS will benefit from the provision that allows U.S. cargo carriers to establish hubs within China, which will be granted a high level of operating flexibility.** The freedom to operate hubs in the country will be a key strategic advantage for FedEx and UPS as they seek to expand their presence and continue growth in the country. In addition, cargo carriers will be able to connect to third countries so that, for example, UPS will be able to serve the thriving China−Japan trade route.
Source: http://www.commentwire.com/commwire_story.asp?commentwire_ID =5735

[Return to top]

Agriculture Sector

17. *June 22, Oster Dow Jones Commodity News* — **Mexico rule halts imports. A procedural change enacted June 17 to Mexico's import regulations has effectively halted U.S. shipments of hogs and sheep into the country, a U.S. Department of Agriculture (USDA) spokesman said Monday, June 21.** USDA spokesman Ed Loyd said the change in Mexican regulations calls for inspections of the U.S. hogs and sheep to now be done inside Mexico but that Mexico does not yet "have the facilities ... set up to do that." Said the USDA's Loyd: "USDA has protested this action to Mexican congressional members who mandated the change and Mexican officials responsible for enforcing this new requirement." He called the Mexican rule a "non−tariff trade barrier" and stressed that the USDA is working to get it lifted "as quickly as possible."
Source: http://www.agprofessional.com/show_story.php?id=25809

18. *June 21, Food and Drug Administation* — **Statement on dairy cattle deaths in Washington state. The Food and Drug Administration (FDA) Monday, June 21, confirmed that it is investigating reports that at least three dairy cattle have died after exposure to a toxic substance on a farm in Enumclaw, WA, approximately 50 miles southeast of Seattle.** FDA’s Seattle District and the FDA Office of Criminal Investigations are working closely with the Federal Bureau of Investigation, the Department of Homeland Security, the U.S. Department of Agriculture, and the King County, WA, Sheriff’s Office, as well as authorities from the Washington State Department of Agriculture and Public Health −− Seattle and King County. At this point the incident appears to be isolated, involving fewer than 20 dairy cattle, although not all of the exposed cattle became ill. No milk from the sick animals has entered the food supply. FDA and FBI investigators visited the farm over the weekend and again Monday, June 21. Tissue samples from a cow that died Saturday, June 19, are being analyzed at FDA’s Forensic Chemical Center.
Source: http://www.fda.gov/bbs/topics/news/2004/NEW01079.html

19.

June 21, Reuters — **Peru reports foot−and−mouth outbreak. Peru has reported its first outbreak since 2000 of the highly contagious foot−and−mouth disease, saying eight infected cattle and 80 animals in contact with them have been slaughtered and more were being killed.** "It's been a fairly light outbreak, and now it is under control," Jose Ochoa of the National Service of Agrarian Health (SENASA) said. Ochoa said the three establishments in Lurin, south of Lima, where the disease was detected, had been sealed off. Foot−and−mouth disease affects cloven−hoofed animals and although Peru does not export beef, it is keen to recover its foot−and−mouth free status because the virus can be transported, for example, with fruit and vegetables. That could potentially affect Peru's bid for a free−trade treaty with the U.S., which is free of the disease. Ochoa said "more animals that were close (to those infected) are being slaughtered now." He said it was unclear how many would be killed, but it would be "many more." Some 800 other cattle had been in contact with those infected, he said.
Source: http://203.210.108.22/dailynewsstory.cfm/newsid/25607/story. htm

[Return to top]

Food Sector

20. *June 22, Associated Press* — **Toxic chemical found in cow's milk.** Young children and pregnant women who drink milk from California cows may be exposed to unsafe levels of a toxic chemical used in rocket fuel, according to a new study by an environmental group. The study released Tuesday, June 22, by the Environmental Working Group (EWG), a research and advocacy organization based in Washington, DC. Researchers are divided about the effects of perchlorate on mental development and what exposure levels are safe. **The Environmental Protection Agency advocates a standard of just one part per billion.** The new study on milk was based on laboratory tests the EWG commissioned as well as unreleased tests by the California Department of Food and Agriculture. **The EWG tests, conducted by researchers at Texas Tech University, found the chemical in 31 of 32 samples from milk purchased at grocery stores in Los Angeles and Orange counties. The average level of the chemical was 1.3 parts per billion, The EWG said the Food and Agriculture Department tests found an average level of 5.8 parts per billion of perchlorate in 34 samples it tested from milk silos in Alameda, Sacramento, and San Joaquin counties.**
Source: http://www.mlive.com/newsflash/lateststories/index.ssf?/base /national−1/1087907647166790.xml

21. *June 21, Associated Press* — **Warehouser admits selling tainted meat. The owner of a now−closed food processing and distribution company pleaded guilty Monday, June 21, to selling thousands of pounds of meat that had been contaminated by rodents.** Lihn Vi Lam, owner of Big Bird Poultry, waived her right to a federal indictment and pleaded guilty to a charge of offering adulterated food for sale. Big Bird Poultry sold cuts of chicken and other meat to restaurants and hotels in the Kansas City, MO, area. **U.S. Attorney Todd Graves said Lam admitted storing 6,935 pounds of beef, pork, and lamb in such unsanitary conditions that it became infested with rodents and their hair and fecal matter.** She said she knew about the infestation and that a plant manager would sweep away rodent droppings before routine visits by agricultural inspectors. Officials discovered the contamination in April 2001 and ordered the meat and 22,780 pounds of chicken destroyed.
Source: http://abcnews.go.com/wire/US/ap20040621_1974.html

[Return to top]

Water Sector

22. *June 22, Salt Lake Tribune (UT)* — **Federal water grants.** The U.S. Department of Interior's "Water 2025" program, which is aimed at avoiding conflict over water in the Western U.S. during the next two decades, has begun issuing funding. **In this first round of grants, Interior Secretary Gale Norton awarded more than four million dollars to 19 projects worth $39 million in 10 Western states.** In a prepared statement, Norton said the Water 2025 grant program will "help prevent crises and conflict" over limited water resources in the 10 Western states. "Watersheds in the West are experiencing a worsening of chronic water supply shortages because of growing populations and heightened competition for a finite supply." **Interior has asked Congress for a $21 million Water 2025 appropriation for next year,** said department spokesperson Trudy Harlow.
Source: http://www.sltrib.com/2004/Jun/06222004/utah/177784.asp

[Return to top]

Public Health Sector

23. *June 22, BBC* — **Polio epidemic warning for Africa. West and Central Africa is on the brink of the largest polio epidemic in recent years, experts have warned.** The Global Polio Eradication Initiative says thousands of children are at risk of paralysis. Five times as many children in the region have been hit by polio in 2004 as last year. The upsurge has been linked to a suspension of the vaccination program in northern Nigeria. Last month a child was paralyzed by polio in Darfur −− the first case in Sudan for three years. **This means that ten countries have now been reinfected with the virus since the Nigerian state of Kano stopped immunizations for eight months last year after Islamic elders voiced concerns about vaccine safety.** Since immunizations stopped 237 cases have been reported across West and central Africa, including 197 in Nigeria, compared to a total of 49 cases for the same period last year.
Source: http://news.bbc.co.uk/1/hi/health/3829129.stm

24. *June 22, Public Library of Science* — **Inadequate vaccines can help breed more vicious malaria strains.** Vaccination programs could create conditions which promote the evolution of virulent strains of malaria, according to a laboratory−based study of the malarial parasite Plasmodium in mice. The findings, published in the journal, PLoS Biology, are likely to spark debate among public health groups seeking to curb the disease, which claims up to two million lives each year. Vaccines are designed to protect people by boosting the immune system to kill parasites but, unless a malaria vaccine leads to the death of every single parasite, the ones that survive are likely to be the nastiest. **"Many questions remain, but these results make a strong case that vaccine development aimed at containing infectious pathogens would do well to consider the evolutionary implications, or increased pathogen virulence could be an unintended consequence,"** said researcher Margaret Mackinnon, of the University of Edinburgh's Institute of Cell, Animal & Population Biology.

Source: http://www.eurekalert.org/pub_releases/2004−06/plos−ivc06150 4.php

25. *June 21, Federal Computer Week* — **Government primes multipronged effort to detect and counter bioterrorism attacks.** The signs of a bioterrorist attack −− especially in the immediate aftermath −− can be difficult to ascertain. To tell if an outbreak of illness is the result of a biological attack, scientists need to compile and analyze certain information such as who got sick, when, where, and with what. Prompt analysis could help pinpoint the source of any outbreak, predict its course and help stem its spread. The needed technological tools, however, are still under development. **The Bush administration has proposed $6.98 billion in fiscal 2005 for biodefense−related programs across the federal government. That includes $274 million for a Bio−Surveillance Program Initiative. According to the Department of Homeland Security (DHS) officials, the initiative will, among other things, require DHS to create a system that will integrate a broad variety of bioinformatics data from across the government.** Scientists at the Walter Reed Army Institute of Research in Silver Spring, MD, are using existing military medical records and newly developed software in hopes of creating early notification systems for an epidemiological outbreak. The work at Walter Reed is being augmented at the U.S. Centers for Disease Control and Prevention. The BioSense Project adds anonymous civilian medical data to the gathered military data.
Source: http://www.fcw.com/supplements/homeland/2004/sup2/hom−bugs−0 6−21−04.asp

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *June 22, Associated Press* — **New York City doormen get anti−terrorism training.** Building superintendents and doormen in New York City are receiving anti−terrorism training under a program developed with the help of the Police Department. While the September 11 attacks vividly illustrated the vulnerabilities of office high−rises and government buildings, security experts have more recently raised concerns about apartment houses. **Terrorists "may be moving from high−visibility targets like the Pentagon" to softer targets such as apartments,** said Matthew Levitt, a former FBI anti−terrorism analyst and now a fellow at the Washington Institute for Near Eastern Policy. **The workers will receive four hours of classroom training. Among other things, they will be warned to be on the lookout for cars or trucks that are parked near buildings for a long time, or that have no license plates; for anyone who takes pictures of the building or lingers too long outside; and for new tenants who move in with little or no furniture.** Doormen who routinely sign for packages and accept deliveries for tenants are also taught to watch for parcels with no return address or too much postage. The doormen and supers will also get lessons on how to recognize phony IDs and documents and will be taught how to respond to bomb threats and how to contain biological and chemical agents.
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−a

partment−vigilance,0,7664759.story?coll=sns−ap−nation−headli nes

27. *June 21, GovExec.com* — **9/11 communication failures still baffle FAA, Defense officials.** Officials from the Federal Aviation Administration (FAA) and Department of Defense last week told the federal commission investigating the September 11 terrorist plot that they are still trying to understand how communications broke down between them on the day of the attacks. **An interim report from the commission's staff revealed a communication failure between FAA headquarters and the Pentagon's National Military Command Center (NMCC) as the attacks unfolded.** Among many problems, poor communication meant the military mistakenly thought American Airlines Flight 11, which crashed into the north tower of the World Trade Center, was headed to Washington, DC. "The most frustrating after−the−fact scenario for me to understand and to explain is the communication link on that morning between the FAA operations center and the NMCC," said Monte Belger, who was the acting FAA deputy administrator when the attacks occurred. "I know how it's supposed to work, but I have to tell you it's still a little frustrating for me to understand how it actually did work on that day."
Source: http://www.govexec.com/dailyfed/0604/062104c1.htm

[Return to top]

Information Technology and Telecommunications Sector

28. *June 22, SearchSecurity.com* — **Vulnerability in Symantec Enterprise Firewall. A hole in Symantec's Enterprise Firewall could be exploited by a malicious person to poison the domain name service (DNS) cache**, IT security firm Secunia said in an advisory. A fix is not yet available. "If a DNS cache is poisoned, one can no longer trust any Website or host based on its domain name," said Thomas Kristensen of Secunia said. He added the problem "is an issue for system administrators, not normal private users." **When acting as a caching DNS server, the integrated DNS proxy reportedly trusts any answer received from a DNS server without checking that it actually corresponds to a query or is valid**, Kristensen said. This can be exploited to insert fake information in the DNS cache, which can be used to direct users to malicious Websites or just prevent them from accessing certain Websites. The problem has been reported in versions 7.0.4 and 8.0 for Solaris. Other versions may also be affected. Symantec has been informed of the problem and is investigating it, the advisory said. For now, IT administrators are advised not to use the DNS proxy until a fix is available. Secunia advisory: http://secunia.com/advisories/11888/
Source: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci989627,00.html

29. *June 22, SearchSecurity.com* — **Vulnerability in ZoneAlarm Pro.** An attacker could use a bypass vulnerability in Zone Lab's ZoneAlarm Pro software to lure users to malicious sites and there is currently no workaround, according to IT consulting firm Kurczaba Associates. The firm said that the problem was uncovered during testing on a Windows XP Professional machine running ZoneAlarm Pro 5.0.590.015. The machine was also equipped with Internet Explorer 6.0 and all patches. **The problem lies in ZoneAlarm Pro's mobile code filter, which integrates with Internet Explorer. The filter blocks potentially dangerous Web objects such as ActiveX, Java Applets, and certain MIME objects. It also blocks out any**

"application/*" MIME type. According to the advisory, it does not filter content on the secure sockets layer (SSL), a commonly used protocol for managing the security of a message transmission on the Internet. "A malicious person could lure a ZoneAlarm Pro user to a malicious SSL site with dangerous mobile code content; and ZoneAlarm Pro would not filter the mobile code." Kurczaba advisory:
http://www.kurczaba.com/securityadvisories/0406214.htm
Source: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci989633,00.html

30. *June 22, Washington Post* — **Carlyle group embraces Telecom.** The Carlyle Group said Monday, June 21, it would buy one of Japan's largest wireless data providers. **Carlyle led the team purchasing Tokyo−based DDI Pocket for $2.03 billion. Carlyle will own 60 percent of the company, with wireless handset maker Kyocera Corp. owning 30 percent. The seller, Japan's KDDI Corp., the second−largest telecommunications company in Japan, will retain a 10 percent interest.** The group also has a piece of the $4.3 billion buyout of satellite network owner PanAmSat Corp., which is expected to close this summer. Also pending is Carlyle's $1.7 billion purchase of Verizon Communications Corp.'s local phone business in Hawaii. And 10 months ago, Carlyle was part of a group that bought phone directory company Dex Media Inc. from Qwest Communications International Inc. for $7.05 billion. Carlyle plans to take Dex public in a $1.5 billion stock offering later this year.
Source: http://www.washingtonpost.com/wp−dyn/articles/A58968−2004Jun 21.html

31. *June 22, US−CERT* — **Technical Cyber Security Alert TA04−174A: Multiple Vulnerabilities in ISC DHCP 3. Two vulnerabilities in the ISC DHCP allow a remote attacker to cause a denial of the DHCP service on a vulnerable system. It may be possible to exploit these vulnerabilities to execute arbitrary code on the system**. For both of the vulnerabilities, only ISC DHCP 3.0.1rc12 and ISC DHCP 3.0.1rc13 are believed to be vulnerable. VU#317350 is exploitable for all operating systems and configurations. All versions of ISC DCHP 3, including all snapshots, betas, and release candidates, contain the flawed code. However, versions other than ISC DHCP 3.0.1rc12 and ISC DHCP 3.0.1rc13 discard all but the last hostname option provided by the client, so it is not believed that these versions are exploitable. These issues have been resolved in ISC DHCP 3.0.1rc14:
http://www.isc.org/index.pl?/sw/dhcp/
Source: http://www.us−cert.gov/cas/techalerts/TA04−174A.html

32. *June 21, Techworld* — **IBM faces highly critical support security hole.** Hackers could use two IBM ActiveX controls designed for automated PC support to attack PCs through the Internet Explorer browser, according to security firm eEye. **The company found flaws in the eGatherer 2.0.0.16 and acpRunner 1.2.5.0 ActiveX controls−−the first of which is installed by default on many IBM PCs−−that could allow attackers to write malicious files anywhere on a computer's hard disk via a special Web page**. Because the controls are signed by IBM, users who agree to "trust" IBM components could be compromised, eEye said in advisories last week. The company published example exploits for both controls. IBM has released a fix for the problem:
http://www−306.ibm.com/pc/support/site.wss/document.do?lndoc id=MIGR−51860 eEye advisory: http://www.eeye.com/html/research/advisories/AD20040615B.htm l
Source: http://www.techworld.com/security/news/index.cfm?newsid=1770

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: The Korgo virus is currently undergoing many variants in an effort to spread on the Internet. Part of the Korgo payload causes infected systems to download code from hacker−controlled websites. As these malicious websites are located and shut down by security personnel, new websites are created to host the malware. Ensure that your antivirus is up to date and check your logs for port 113 authentication requests to locate infected systems.

Current Port Attacks

Top 10 Target Ports	9898 (dabber), 445 (microsoft−ds), 5554 (sasser−ftp), 135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 3127 (mydoom), 1023 (Reserved), 1433 (ms−sql−s), 80 (www) 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

33. *June 23, Associated Press* — **Iran orders release of British sailors. Iran will release eight British sailors whose military patrol boats entered Iranian waters, after an investigation revealed the incursion was a mistake, Iran and Britain said Wednesday, June 23.** The decision to free the eight, who have been held since Monday, June 21, defused a brewing diplomatic crisis between London and Tehran. Iran had earlier threatened to prosecute the men, while Britain insisted they had simply strayed off course while working as part of the U.S.−led coalition in Iraq. Foreign Minister Kamal Kharrazi said they would be released later Wednesday, June 23. British Prime Minister Tony Blair's official spokesman said Britain had been told the same thing. The men were detained Monday, June 21, in the Shatt−al−Arab waterway, which runs along the Iran−Iraq border and is known in Iran as the Arvand River. Iran said the vessels were about a half−mile inside Iranian territorial waters.
Source: http://story.news.yahoo.com/news?tmpl=story&u=/ap/20040623/ap_on_re_mi_ea/iran_british_boats&cid=540&ncid=716

34. *June 22, New York Times* — **Rebel raid near Chechnya is said to kill at least 75 people.** An overnight raid by heavily armed militants in a southern Russian republic neighboring Chechnya killed as many as 75 people and wounded dozens more before the fighters withdrew with minimal losses and a cache of captured weapons, officials said Tuesday, June 22. **The raid,**

which began late Monday night with a series of attacks against police and security posts across the republic, Ingushetia, was the largest attack by Chechen separatist rebels outside Chechnya since 1999. President Vladimir Putin met with his law enforcement deputies in the Kremlin Tuesday. He vowed to retaliate for the raid. The fighting killed Ingushetia's acting interior minister, Abukar Kostoyev, and his deputy. In all, some 200 militants were believed to have taken part in the attacks. New fighting was reported Tuesday afternoon near Galashki, a small village in Ingushetia, where at least some of the militants appeared to be making their way through the rugged Caucasus foothills southeast of Nazran toward Chechnya. They were driving stolen trucks and cars loaded with ammunition, weapons and, possibly, explosives, the officials said.
Source: http://www.nytimes.com/2004/06/22/international/europe/22CND−RUSS.html?ex=1088568000&en=15ab978abdbb08f0&ei=5062&partner =GOOGLE

[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.