Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 08 August 2003

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

Daily Overview

- The Bulletin reports Oregon's Governor signed two bills into law on Wednesday, designed to help thwart the state's rising tide of identity theft. (See item 6)
- The Associated Press reports a leaking freight train spilled hazardous chemicals in Washington, DC on Thursday, during the height of the afternoon rush hour. (See item 10)
- The Mercury News reports that hackers exploiting a vulnerability in Microsoft's Windows operating system infected thousands of desktop computers at Stanford University, Thursday. (See item 26)
- The New York Times reports a car bomb that ripped apart the Jordanian Embassy in Baghdad Thursday, August 7, killing 11 and wounding 65, has brought terrorism to the heart of Iraq's capital, targetting a vulnerable and undefended structure. (See item 31)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; 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 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. *August 07, The Atlanta Journal−Constitution* — **Russian oil probe worries the West. Russia's biggest oil company, Yukos, and the company's chairman, 40−year−old billionaire Mikhail Khodorkovsky, are the subjects of a legal crackdown that seems to**

have the backing of the Kremlin. The campaign has Western analysts worried that Russia is backsliding into the kind of Byzantine power struggles of the 1990s that plagued the budding democracy. It started July 2 when Platon Lebedev, a close associate of Khodorkovsky and the head of Menatep, a company that controls about 60 percent of Yukos, was arrested on fraud charges over his involvement in the privatization of a fertilizer company in 1994. From there, the legal problems for Yukos and its related enterprises blossomed to include a murder charge against the company's security director, Alexei Pichugin, allegations that Lebedev falsely registered a company in a city where it did not do business, and police raids on the oil company's Moscow offices. **Khodorkovsky has promoted oil exports to the United States and a new pipeline to Russia's far north.** President Vladimir Putin doesn't necessarily oppose these things, he'd just rather be the one promoting them, analysts say. Khodorkovsky was perceived as stepping into the political arena and trying to shape Russian foreign policy. Since the crackdown on Yukos, the company has lost about $7 billion in value.
Source: http://www.ajc.com/news/content/news/0803/07russia.html

2. *August 07, Anchorage Daily News (AK)* — **Technology could help move stores of stranded natural gas. An experimental plant at Nikiski, AK, designed to turn natural gas into a liquid form, began operations on Sunday, July 27. The goal of the $86 million gas−to−liquids (GTL) plant is to test secret technology that could someday help bring massive global stores of stranded gas, such as that on the North Slope, to market. The estimated 35 trillion cubic feet of North Slope gas is stranded for lack of a long and expensive pipeline to carry it out.** At least some of the world's stranded gas could be carried in existing oil pipelines, provided the gas could be economically converted to a stable liquid, which is what the Nikiski demonstration plant is trying to do. It is turning Cook Inlet natural gas into about 100 barrels a day of clear liquid called synthetic crude oil, also known as syncrude or white crude. The plant eventually will ramp up to about 250 barrels per day, said Dave MacDowell, spokesman for the company responsible for the experiment. MacDowell cautioned that the plant is not a precursor to moving large, commercial quantities of North Slope gas down the trans−Alaska oil pipeline. Rather, the company is trying to prove the technology works, and can be used anywhere in the world.
Source: http://www.adn.com/business/story/3611675p−3643649c.html

[Return to top]

Chemical Sector

3. *August 07, WOKR−TV 13 Rochester* — **Chemical spill in Palmyra, New York.** Haz−mat crews from Rochester and Buffalo worked through Wednesday night into Thursday cleaning up a chemical spill at Garlock Inc., a manufacturing plant on Division Street in Palmyra. **A company spokesperson said that an unknown amount of diluted sulfuric acid spilled around 8:00 p.m. Residents from two nearby streets were evacuated to the fire station to avoid contact with fumes.** According the company, which manufactures gaskets and seals, this was a minor spill.
Source: http://www.wokr13.tv/news/local/story.aspx?content_id=42474328−87DC−4CFD−9C59−404A10A2809B

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *August 07, BBC News* — **Bank fined over identity lapse. One of Northern Ireland's largest banks, the Northern Bank, has been fined £1.25m (USD$2,012,375) for failure to make proper checks on its customers.** The fine was imposed by the Financial Services Authority (FSA), under rules designed to prevent money laundering. **The Northern Bank admitted on Thursday, August 6, that it had failed to keep proper records of details which customers opening new accounts are required to provide.** Regulations which call for customers to give two forms of identification − photographic identification and proof of address, such as a utility bill − were breached. The FSA said the size of the fine demonstrated the importance it attaches to minimizing risk of regulated firms being used for purposes connected to financial crime.
Source: http://news.bbc.co.uk/1/hi/northern_ireland/3131897.stm

5. *August 07, Continuity Central* — **U.S. agencies publish Basel Accord consultation documents. The four U.S. federal bank and thrift regulatory agencies (the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and the Office of Thrift Supervision) have announced the publication of joint Federal Register notices and requests for comment on two interagency documents related to the proposed implementation of the new Basel Capital Accord in the United States.** The two documents detail the agencies' current views on a proposed framework for implementing the revised Capital Accord in the United States, and draft supervisory guidance and expectations on corporate credit and operational risk management. Comments on the two documents will be accepted up to November 3rd, 2003.
Source: http://www.continuitycentral.com/news0437.htm

6. *August 06, The Bulletin (OR)* — **Oregon governor signs bills to thwart identity theft. The Governor of Oregon signed two bills into law on Wednesday, August 6, designed to help thwart the state's rising tide of identity theft. The legislation would increase penalties for possession of equipment used to manufacture false identification cards and create a crime of possessing a personal identification card for a fictitious person.** The Federal Trade Commission's Identity Theft Data clearinghouse ranked Oregon 10th in the nation for 2002, with 2,200 cases reported to the FTC that year, the governor said. Under the new laws, it would be a Class C felony to possess a device used to manufacture or print drivers' licenses or permits, employee identification cards or credit cards if the person also can be shown as intending to commit a crime. A Class C felony is punishable by up to five years imprisonment, a $100,000 fine, or both. Underage minors who create fake ID's to buy cigarettes or alcohol are exempted from the law.
Source: http://www.bendbulletin.com/news/story.cfm?story_no=10360

7.

August 06, The New Indian Express — **ATM hacker in India was wanted by the FBI. Police in Chennai, India, arrested Deepak Prem Manwani, for allegedly stealing money from ATM machines.** It started when he was browsing the internet and was attracted to a site which offered him assistance in breaking into the ATMs. His contacts, somewhere in Europe, were ready to give him credit card numbers of a few American banks for $5 per card. The site also offered the magnetic codes of those cards, but charged $200 per code. **To get PIN's of card holders, the operators of the site created a new website which resembled that of a reputed telecom company's. That company has millions of subscribers. The fake site offered the visitors to refund $11.75 per subscriber, which, the site promoters said, had been mistakenly collected from them. Believing that it was a genuine offer from the telecom company in question, several subscribers logged on to the site to get back the money, but in the process parted with their PINs.** On receipt of large−scale complaints from the billed credit card users and banks in the United States, the FBI started an investigation into the affair and also alerted the CBI in New Delhi that the international gang had developed some links in India too.
Source: http://www.newindpress.com/Newsitems.asp?ID=IET20030805142349&Title=Southern+News+−+Tamil+Nadu&rLink=0

[Return to top]

Transportation Sector

8. *August 07, New York Times* — **U.S. is inspecting overseas airports for missile threats.** The Bush administration has dispatched teams of aviation safety investigators to Iraq and to major capital cities in Europe and Asia to determine if their commercial airports can be defended against terrorists who might try to shoot down passenger planes using shoulder−fired missiles, senior American officials say. **The inspections at airports in the Iraqi cities of Baghdad and Basra −− as well as in Athens, Istanbul, Manila and several other foreign capitals where American air carriers have regularly scheduled flights −− are part of the administration's response to recent intelligence reports suggesting that a terrorist attack using small heat−seeking missiles may be imminent, probably overseas. Intelligence agencies say al Qaeda has dozens of the small missiles, many of them Stingers made in the United States, left over from the American−led effort to help Muslim guerrillas oust the Soviet Union from Afghanistan in the 1980's.** Hundreds of other shoulder−fired missiles, including Stingers and Russian SA−7's, which are designed for portability and can weigh as little as 30 pounds apiece, are believed to be in the hands of other terrorist organizations and rebel groups around the world.
Source: http://www.nytimes.com/2003/08/07/international/worldspecial 2/X07MISS.html?hp

9. *August 07, Newsday.com* — **Ferries: no new sense of alarm. Despite a new warning from the Coast Guard that ferry services nationwide may be under surveillance by terrorist groups, some Long Island operators said customers don't need to worry because security has been tight since the September 11 attacks**. "We will never be as relaxed as we were before September 11," said Fred Hall, vice president and general manager of the Bridgeport and Port Jefferson Steamboat Co., which ferries up to one million people a year. While recognizing the importance of the security concerns, some Long Island providers said ferryboats don't carry any greater risk than other forms of transportation. **The recent warning asks ferry operators**

and passengers to report suspicious packages, activities and persons to the U.S. Coast Guard. Items that appear out of the ordinary, such as unattended suitcases, and odd behavior should be reported, said Tom Sperduto, a spokesman with the Coast Guard in New York City. **The Coast Guard recommends ferry operations increase the visibility of security personnel and check employees and passengers for proper identification, among other measures.** More than half a dozen Long Island ferry services shuttle cars and passengers between Connecticut, Rhode Island and Fire Island, Shelter Island and Block Island.
Source: http://www.newsday.com/news/local/longisland/ny−liferr073404889aug07,0,3251553.story?coll=ny−linews−headlines

10. *August 07, Associated Press* — **Chemical spill in Washington, DC. A leaking freight train spilled hazardous chemicals Thursday during the height of the afternoon rush hour in the city.** One car of the 138−car CSX train developed a leak in an unpopulated area near the Washington Navy Yard shortly after 5 pm, DC Fire and EMS spokesman Alan Etter said. **The train was carrying sodium hydroxide, a corrosive chemical that can cause severe eye and respiratory irritation. The leak appeared to be in a drain valve on the bottom of a tanker car, Etter said.** No one was injured and no buildings were evacuated, Etter said.
Source: http://www.wusatv9.com/news/news_article.asp?storyid=21351

11. *August 06, Fleet Owner* — **Trucking security still stuck in slow lane. Efforts to secure the trucking industry and the freight transport infrastructure could be stuck in low gear for some time to come, according to a noted security expert.** "We've made great headway in the areas of research and development and in identifying security problems and solutions when it comes to the freight industry and trucking as a whole," Bob Bevelacqua, executive VP for Reston, VA−based homeland security consulting firm WDC3 Group, told Fleet Owner. **Bevelacqua said the cost of implementing security measures is what's really dissuading the industry both now and in the future.** "Trucking companies will only add security technology if it is mandated by the government or if they can afford to do it," he explained. "Incentives such as freezing or reducing insurance premiums and speeding up border crossings will drive security adoption by the industry." **Bevelacqua warned that the longer the industry and the U.S. as a whole goes without experiencing a terrorist event like 9/11, the less pressure there is to beef up security.** "Right now, homeland security isn't a priority −− making money and stabilizing company finances is," he added. "I am afraid that the false sense of security we have that a second September 11−style attack hasn't yet occurred could hurt the industry down the road."
Source: http://industryclick.com/magnewsarticle.asp?newsarticleid=2691756&magazineid=107&SiteID

12. *August 06, Associated Press* — **Dozens of passengers injured after aircraft shaken by turbulence. A Lufthansa jet was shaken by severe turbulence over the Atlantic on Wednesday, and as many as 35 people were hurt, officials said. Between seven to 10 people required hospital treatment when the plane landed at Bush Intercontinental Airport, its final destination.** The injuries were not thought to be serious. "They were tossed around a lot. Bags (from overhead bins) may have fallen on them," said Ernie DeSoto, spokesman for the airport system. Lufthansa Flight 440, which originated from Frankfurt, Germany, was over the Atlantic when it began experiencing "some pretty bad turbulence," DeSoto said. **The wide−body plane, with 250 people on board, landed Wednesday**

afternoon in Houston, where it was met by several ambulances and fire trucks. Besides those taken hospitals, about 25 passengers needed first aid treatment at the scene. **Initial reports also said the plane suffered some structural damage, DeSoto said.**
Source: http://www.cnn.com/2003/US/Southwest/08/06/plane.turbulence. ap/index.html

[Return to top]

Postal and Shipping Sector

13. *August 07, DM News* — **Potter: none immune to postal reform.** Postmaster general John E. Potter warned mailers yesterday that the reforms recommended by the presidential postal commission would affect everyone in the mail community. Potter said it would be "premature" for any sector of the community to assume that it was immune to the impact of the commission's proposed reforms. During the meeting, officials pointed out signs that the U.S. Postal Service (USPS) was moving toward fiscal health. **Civil service retirement reform legislation passed by Congress earlier this year corrected and reduced the postal service's annual payments into the federal civil servant retirement system, enabling the USPS to pay down its debt**, said Richard Strasser, the USPS' chief financial officer. USPS has made a $3.5 billion payment this fiscal year, with another $2.6 billion to follow next year. **USPS will convert its long−term debt into short−term debt**, paying the cost of the transaction over the next 18 months, Strasser said. **The refinancing should reduce the postal service's annual interest payments from $330 million to $50 million, resulting in a significant benefit to postal customers**, he said.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2470 4

14. *August 06, Pittsburgh Post Gazette* — **Anthrax detection system to stay in Pittsburgh. An anthrax detection system being tested by the U.S. Postal Service in Pittsburgh, PA, will be a permanent fixture. Pittsburgh was one of the 14 cities to begin a four−week test of the biohazard detection system last month.** The system operates in conjunction with mail canceling equipment and continuously collects air samples as letters move through the equipment. Samples are then tested about once an hour for materials that might be anthrax. As the four−week test draws to a close, **Postal Service officials have decided to keep the machines operating in Pittsburgh, Cleveland, and Lancaster.** The system is also being used at a Baltimore, MD mail sorting facility, where it has been in place for more than a year. **Next year, the Postal Service could install the system at all 282 mail sorting facilities across the country.** At that time, the Pittsburgh plant's system could be expanded; the detection system now tests air samples from only one of the facility's eight canceling machines.
Source: http://www.post−gazette.com/localnews/20030806anthrax0806p2. asp

[Return to top]

Agriculture Sector

15. *August 07, Augusta Chronicle* — **Terrorism affects peach farms' work.** Since the September 11 attacks, concern about the vulnerability of America's food supply is on the rise. **Chalmers Carr, a peach farmer in Edgefield, SC, has joined a growing number of South Carolina**

and Georgia growers who are stepping up sanitation and security measures. They also are seeking a seal of approval from independent auditors to satisfy an increasing number of grocery store chains looking for assurances of product safety. **In Carr's case, that means adding a $100,000 wireless computer system that allows workers to log each bin of peaches as it leaves the orchard on hand−held computers**. That isn't the only measure growers are taking to ensure their fruit is free of bacteria and pesticide residue. At the insistence of major retail chains, **growers in Georgia and South Carolina also are undergoing audits by independent labs that measure everything from the amount of chlorine in their wash water to whether workers wear hair nets and wash their hands after using the restroom.**
Source: http://www.augustachronicle.com/stories/080703/met_221−7206. 000.shtml

16. *August 06, Wisconsin Ag Connection* — **U.S. offers Japan beef verification plan. The United States has proposed a third−party audit verification program to monitor U.S. beef processors as a compromise with Japan's demand that U.S. exports be labeled as not containing beef from Canada, OsterDowJones Commodity News (ODJ) reported Monday.** Despite the fact that four weeks ago Japanese officials maintained they would accept nothing less than rigid new labeling regulations, they have expressed approval of the compromise proposal, U.S. officials told ODJ. The U.S. proposal was derived from a program already being run by the U.S. Department of Agricluture's Agriculture Marketing Service which requires meat processors to "get their written manufacturing processes confirmed through independent, third party audits."
Source: http://www.wisconsinagconnection.com/story−national.cfm?Id=8 45&yr=2003

[Return to top]

Food Sector

17. *August 05, Western Producer* — **CFIA looking to extend reach. In the aftermath of the bovine spongiform encephalopathy (BSE) crisis and with the constant threat of other food sector flare−ups or bioterrorism, the Canadian Food Inspection Agency (CFIA) will be asking the federal government for more money and more power to police the border**, says the agency's president Richard Fadden. Fadden said he will be asking for as much as $20 million in extra funding this year, in large part to pay for overtime bills and extra expenses run up after the May 20 announcement that one case of BSE had been found in Alberta. But the request for more inspection authority predates BSE. It flows from the terrorist attacks of September 11, 2001, in the U.S. "We think we have to give ourselves a variety of new powers to deal with border issues that didn't exist before 9/11," Fadden said. **CFIA argues that greater security is needed at the border, including the ability to designate certain ports of entry as the only places certain types of goods can be imported**. "We want to be able to stop and test. We want to deal in all commodities. If there is a crisis, it would be useful to be able to concentrate on one border point per province."
Source: http://www.producer.com/articles/20030731/news/20030731news1 3.html

[Return to top]

Water Sector

18. *August 06, Washington Post* — **IG investigates EPA. The Environmental Protection Agency's (EPA) inspector general (IG) is investigating whether the agency is deliberately misleading the public by overstating the purity of the nation's drinking water**. The inquiry was launched June 18, five days before **the EPA released the "Draft Report on the Environment," which stated that "94 percent of the population served by community water systems were served by systems that met all health−based standards." Internal agency documents, however, show that EPA audits have suggested that the percentage with safe drinking water is much lower, 79 to 84 percent in 2002.** EPA officials said the draft report and other public documents routinely add a caveat stating, "underreporting and late reporting of data affect the accuracy" of the calculations. The EPA bases its statements and documents about safe drinking water on data collected by states from their utilities for about 100 contaminants and pollutants. Peter E. Shanaghan, chief of staff for the EPA's Office of Ground Water and Drinking Water, said the agency first became aware of data collection problems when several utilities suggested in 1998 that their violations were being "overreported." An EPA inquiry, however, found "a degree of underreporting," Shanaghan said.
Source: http://www.washingtonpost.com/wp−dyn/articles/A21544−2003Aug 5.html

[Return to top]

Public Health Sector

19. *August 06, BBC News* — **Breakthrough on Ebola vaccine. Scientists have developed a fast−acting Ebola vaccine that protects monkeys after a single shot. If the vaccine proves similarly effective in humans, it may one day allow scientists to contain Ebola outbreaks quickly.** Ebola virus spreads easily from person to person, causes illness quickly and kills a significant number of the people it infects. There is no treatment for the disease, so preventing the spread of the virus is key to containing outbreaks. If the vaccine proves to be effective in humans, it could be used to block the spread of disease using a strategy known as ring vaccination, a technique which has been successfully employ in the past to stop the spread of smallpox. It involves vaccinating everyone who has been in contact with a person who has the disease and all member's of that person's household. The strategy not only protects people who may have been exposed to the virus but also creates an added barrier of immunity around them, thereby protecting the entire community.
Source: http://news.bbc.co.uk/1/hi/health/3126365.stm

20. *August 06, Government Executive Magazine* — **City hospitals lack equipment to handle bioterror attack. Most urban hospitals do not have sufficient resources to handle a sudden surge in patients seeking medical attention because of a bioterrorist attack**, according to a new report. The availability of medical equipment, including ventilators, isolation beds, and protective suits, varied among the hospitals studied. "If a large number of patients with severe respiratory problems associated with anthrax or botulism were to arrive at a hospital, a comparable number of ventilators would be required to treat them. Yet **half of the hospitals reported having fewer than six ventilators per 100 staffed beds**," the report said. The Health and Human Services Department plans to purchase 2,700 ventilators by September to add to the national stockpile of drugs, vaccines, and medical supplies. **The Bioterrorism Hospital Preparedness Program, administered by HHS, provided approximately $125 million in**

funds last year to eligible states and cities to improve the capacity of hospitals to respond to a bioterrorist attack. Eligible states and cities are slated to receive $498 million for fiscal 2003 through the same program. The report can be found at http://www.gao.gov/new.items/d03924.pdf.
Source: http://www.govexec.com/dailyfed/0803/080603m1.htm

21. *August 06, Scotsman* — **Scientists produce handset to locate DNA. Handheld DNA detectors could be used to spot cancer, bioterrorism agents, and pollutants.** Equipment being developed by NASA would be able to read minuscule amounts of DNA. **The electronic DNA detectors are seen as a potential breakthrough because of their ability to detect DNA from much smaller samples than existing equipment. They would also substantially cut the cost of DNA tests and enable much more widespread screening to take place.** Dr Jun Li, who led the project, said the device had considerable potential. He said: "The main applications will be for handheld devices for quick and simple testing, such as early cancer detection, environmental monitoring, bio−defense and space exploration." **The scientists said the equipment could detect DNA in samples containing only 3.5 million molecules, and probably in those of just a few thousand molecules. By comparison, a drop of water contains trillions of water molecules.** Current DNA detectors replicate the molecules in samples to make them large enough to be tested. Fluorescent dyes are then added, which the sample "read" using lasers. The new device sidesteps the problem of replication by being able to detect extremely small quantities of DNA.
Source: http://acs.yellowbrix.com/pages/acs/Story.nsp?story_id=40689231&ID=acs&scategory=Chemicals&

[Return to top]

Government Sector

22. *August 07, Sierra Vista Herald* — **Thefts alter American Border Patrol's timeline, but not its efforts. As the American Border Patrol increases its high−tech inventory to fight what founder and president Glenn Spencer has in the past called an illegal immigrant invasion of the United States, extra care and concern is now the order of the day for the organization. With someone taking electronic equipment and other items critical to supporting satellite transmissions from the group's headquarters,** Sheriff spokeswoman Carol Capas said a complaint was filed in early January about electronic equipment being taken from a van at Spencer's home. Another complaint was made Friday about more high−tech items being taken. **American Border Patrol is in the process of testing and developing sensors, with 30 of them in place on private property to track the foot traffic of illegal immigrants and drug smugglers, he said. Fine−tuning the sensors continues, with the long range goal of eventually putting in 500 of the devices.** The organization also is testing and developing radio−controlled aircraft to be used to spot illegal activities crossing into the United States from Mexico. **The unmanned aircraft have day and night capabilities, and plans are progressing for a larger plane that will be able to carry more equipment and fly for more than two hours,** Spencer said.
Source: http://www.svherald.com/display/inn_news/news7.txt

[Return to top]

Emergency Services Sector

23. *August 07, Times Union (Albany)* — **Alert focuses on electronic devices as Albany International tries out eye scanners.** Amid renewed concerns that terrorists will target airports and planes, new high−tech security procedures are taking off at Albany International Airport. **With help from a Federal Aviation Administration grant, the airport is trying out devices that will scan workers' eyes and confirm their identities before allowing them access to restricted areas. If the limited pilot project is successful, it could be expanded for use by all 268 authority employees at the airport within nine months,** said acting Chief Executive Officer John O'Donnell. **At the same time, the federal Transportation Security Administration here is stepping up scrutiny of CD players, laptops, cameras and other electronic devices in response to a recent government warning that terrorists may try to use such items to conceal weapons or bombs.** TSA screeners at Albany International already can examine electronic items that are packed in checked luggage using equipment designed to detect minute traces of explosives. Checked luggage is routinely opened and examined as part of the airport's security scheme. But now, airport TSA Director Paul Varville said, screeners also may use trace detection systems to check items that travelers plan to carry with them.
Source: http://www.timesunion.com/AspStories/story.asp?storyID=158188&category=REGIONOTHER&BCCode=HOME&newsdate=8/6/2003

24. *August 07, Federal Emergency Management Agency* — **Homeland Security and six New England states to participate in disaster exercise.** The U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) and emergency management teams from six New England States are participating in Operation Yankee this week, one of the largest disaster preparedness exercises ever held in New England. **The two−day exercise, which starts today at the Naval War College in Newport, RI, is designed to enhance and develop federal, state and tribal response, coordination and preparedness for both a natural and man−made disaster.** "The exercise will allow us to work multiple simulated events so that we can improve our coordination and preparedness on a regional scale," said Daniel A. Craig, regional director for FEMA Region I. The exercise will focus on the impending landfall of a category four hurricane along the New England coast. In addition there will be a simultaneous bio−terrorism event in the region. The exercise will play out the first two days of the incident.
Source: http://www.fema.gov/news/newsrelease.fema?id=3964

25. *August 04, Federal Computer Week* — **Maryland's Anne Arundel County leaders believe they can nurture new ideas for homeland security.** The next generation of homeland security and intelligence technologies could come from a nondescript suite of offices tucked inside an ordinary office building in Maryland's capital city. **The Chesapeake Innovation Center in Annapolis, MD, born from a partnership between the National Security Agency and the Anne Arundel Economic Development Corp., opened in June with a mission to nurture small start−up businesses that plan to develop technology for homeland security.**
Source: http://www.fcw.com/fcw/articles/2003/0804/cov−betting−08−04− 03.asp

[Return to top]

Information and Telecommunications Sector

26. *August 07, The Mercury News* — **Hacker attack damages 2,000 computers at Stanford. Officials at Stanford University scrambled Thursday, August 7, to repair the damage from a hacking attack that has infected thousands of campus computers**. Cedric Bennett, Stanford's director of information security services, said unknown hackers had exploited a newly discovered vulnerability in Microsoft's Windows operating system. **About 10 percent of Stanford's 20,000 desktop computers that run Windows were affected**. The attack placed a mysterious bit of computer coding on each of the infected machines, which Bennett said the hackers could later activate. University technicians have disconnected the infected machines, used by students, faculty and staff, from the campus network.
Source: http://www.bayarea.com/mld/mercurynews/news/local/6479603.ht m

27. *August 06, York Daily Record* — **Feds want Internet fraud complaints.** In an attempt to shut down fraudulent Websites, the FBI, the National White−Collar Crime Center (NW3C) and the Federal Trade Commission have instituted Operation E−Con, "a coordinated initiative focusing on Cyber Crime in the United States and a number of other countries." **Last year, Operation E−Con, which also utilizes the manpower and resources of 43 United States Attorneys' Offices, the Postal Inspection Service, the Secret Service and the Bureau of Immigration and Customs Enforcement, served 70 warrants leading to 130 arrests and over $17 million in property seizures and recoveries**. A quickly escalating problem for Internet users and legal authorities is "spoofing," where a con man masquerades as a trusted Web site using a seemingly valid e−mail address. The unsolicited e−mails direct consumers to a fraudulent site, typically a convincing mock−up of a genuine Web site, where users are asked to update their accounts by revealing bank, credit and personal information. **Scammed Internet users should contact their local police and file a complaint with the Internet Fraud Complaint Center at http://www.IFCCFBI.gov**.
Source: http://ydr.com/story/technology/12067/

28. *August 04, New Scientist* — **Country−coded computer worms may be ahead.** Jonathan Wignall of the UK's Data and Network Security Research Council highlighted techniques that worm creators might use to make their code spread more effectively during a presentation at the security conference Defcon 11 in Las Vegas, NV, on Sunday, August 3. **One of these techniques could also limit a worm's geographic range, which would turn a computer worm into an effective weapon for information warfare, he said. Instead of attacking internet−connected computers at random it could be used to attack a specific country**. After infecting a host computer, a worm normally scans randomly for further machines that could be infected. But Wignall says **a worm could download a prepared list of internet protocol (IP) addresses to attack from a single server or a group of machines. This would prevent duplicate requests being sent to each machine**, a common cause of bottlenecking with existing worm design. Nicholas Weaver, a computer scientist at the University of California in Berkeley says **this is just one way that a worm could, in theory, be used to target a specific country. Another way is to avoid computers running a particular language**, he says.
Source: http://www.newscientist.com/news/news.jsp?id=ns99994016

29.

August 04, Boston Business Journal — **Former Telecast Fiber worker pleads guilty to hacking. A former employee of Telecast Fiber Systems Inc. in Worcester, MA, pleaded guilty Friday, August 1, in federal court to breaking into the company's computer system and deleting valuable files**, according to the U.S. Attorney's office. John Corrado, 35, agreed to pay $10,360, the estimated financial loss suffered by the company. His formal sentencing is scheduled for October 7 where he faces a maximum penalty of one year imprisonment and a fine of $100,000. The U.S. Attorney's office says that **in July 1999, about one month after Corrado had stopped working for the company, he accessed the company's network server using a modem from a remote location**. The files he deleted included those used for research and development as well as those used by sales reps to demonstrate company products. Source: http://boston.bizjournals.com/boston/stories/2003/08/04/dail y11.html

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **PE_VALLA.A** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	445 (microsoft−ds), 80 (www), 137 (netbios−ns), 1434 (ms−sql−m), 113 (ident), 139 (netbios−ssn), 0 (−−−), 41170 (−−−), 25 (smtp), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

30. *August 07, Associated Press* — **Taliban attack kills six Afghan soldiers. Dozens of suspected Taliban fighters attacked a government office in southern Afghanistan early Thursday**, August 7, killing six Afghan soldiers and an Afghan driver for an American aid organization, a provincial intelligence chief said. **The attack was possibly part of a trend involving militants targeting Afghans working for foreign agencies**. The violence occurred in Deshu district, about 110 miles south of Lashkargah, the capital of Helmand province. **At least six Afghans working for the American aid organization Mercy Corps were conducting an agricultural survey in the region and were staying in the building** at the time, said the intelligence chief, Dad Mohammed Khan. Khan said about 40 suspected Taliban fighters drove up in four vehicles, entered the government offices and opened fire. The use of the vehicles was unusual and bold as the militants usually travel on foot, making them less conspicuous. **The Taliban,**

who were ousted in a U.S.−led war on terror in late 2001, have been waging a hit−and−run guerrilla war in the south and east of the country for over a year.
Source: http://www.chicagotribune.com/news/sns−ap−afghan−taliban−att ack,1,4356643.story

31. *August 07, New York Times* — **Embassy blast raises specter of terrorism in Baghdad. The car bomb that ripped apart the Jordanian Embassy in Baghdad Thursday, August 7, killing 11 and wounding 65, has brought terrorism to the heart of Iraq's capital**. This attack was not directed against well−armed American forces but against what the military calls a "soft target," a vulnerable and undefended structure. **The goal was not to alter the military equation but to produce a large number of civilian casualties**. In recent weeks, it has become clear that **American forces are not only fighting remnants of the Saddam Hussein regime, Fedayeen militia and disgruntled Iraqis but also facing a panoply of military and even terrorist factions who appear to see Iraq as a new arena for pursuing their Jihad against America.** American military officials say that **al Qaeda−like fighters−−militants from Syria, Saudi Arabia, Yemen and other nations−−have infiltrated into Iraq from Syria.** The Jordanians discovered Thursday that they were a target as well, possibly because of their low−profile support for the United States.
Source: http://reuters.com/newsArticle.jhtml;jsessionid=YUFSF3JWMFVR CCRBAEKSFFA?type=topNews&storyID=3240530

32. *August 06, Associated Press* — **Software engineer admits aiding Taliban. Software engineer Maher "Mike" Hawash pleaded guilty Wednesday, August 6, to a charge of aiding the Taliban**. In exchange, prosecutors dropped charges of conspiring to levy war against the United States and conspiring to provide material support for terrorism. Hawash, one of the so−called "Portland Seven," will serve at least seven years in federal prison under the deal, which was approved by U.S. Attorney General John Ashcroft. **In an affidavit, the U.S. Attorney's Office accused Hawash, a naturalized U.S. citizen of Palestinian descent, of growing angry with the United States after the September 11, 2001, attacks, then conspiring with co−defendants to join the fight in Afghanistan against U.S. troops**. Hawash accompanied the group as it tried and failed to enter Afghanistan from western China in late fall 2001, according to court documents.
Source: http://www.washingtonpost.com/wp−dyn/articles/A23640−2003Aug 6.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−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

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:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

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. This 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.