



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 20 April 2004

Current Nationwide Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports a commuter train was struck from behind by an empty Amtrak train as they approached Penn Station on Monday morning, and at least 130 people suffered minor injuries. (See item [8](#))
- The Associated Press reports a behavior pattern recognition program is under way at Logan Airport; officials look for odd or suspicious behavior such as heavy clothes on a hot day, loiterers without luggage, anyone observing security methods. (See item [11](#))
- The Associated Press reports Department of Homeland Security Secretary Tom Ridge is forming a new government task force to better coordinate public and private security. (See item [22](#))
- eSecurity Planet reports security researchers are warning of a buffer overflow security flaw in the Linux kernel that can be exploited to lead to privilege escalation attacks. (See item [26](#))

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. *April 19, The Sun Herald (MS)* — **In energy push, companies gather in Gulf.** The furor in Mobile, AL, over ExxonMobil's interest in locating a liquefied natural gas (LNG) terminal in

the Bay has died down somewhat with a recent pitch by a competing company to take the project 11 miles offshore. **As the nation seeks to address its growing energy needs with growing natural gas imports, security fears about liquefied natural gas tankers have stimulated staunch resistance to terminals being located near population centers in Southern California and Maine as well as Mobile. Due to public reaction over the terminals, many energy companies have begun to scan the Gulf of Mexico for a more publicly palatable location** — despite the additional hundreds of millions of dollars locating offshore would mean. A typical onshore site costs about \$600 million to develop. An offshore site could pass the billion dollar mark, said Bob Davis of ExxonMobil. The U.S. Coast Guard, which rules the regulatory domain on the waves beyond has received five permit applications to operate LNG terminals in the Gulf of Mexico. Two companies have received preliminary approval from the U.S. Coast Guard for their Gulf-based projects, but "no licenses have actually been approved yet," said Jolie Shifflet, a Coast Guard spokesperson.

Source: <http://www.sunherald.com/mld/sunherald/8467327.htm>

2. *April 19, Associated Press* — **Tax credit suspension leaves wind energy industry stalled.**

Congress has effectively pulled the plug on the wind energy industry by failing to extend a crucial tax credit, leaving \$2 billion worth of projects on hold across the country. Utilities rely on the tax credit, 1.8 cents per kilowatt-hour, to pick up about one-third of the cost of wind energy they produce. Wind farms that were built when the tax credit was in place receive the credit for 10 years, so existing operations are not affected by the credit's expiration. However, the expiration is holding up new construction. **"The tax credit lapse has brought the industry to a screeching halt," said Mark Haller, owner of Haller Wind Consulting at River Falls in western Wisconsin. Nationally, wind energy provides about 1 percent of the nation's energy.** Legislation to renew the wind energy production tax credit for three years was included in last year's energy bill, but that bill failed to get through Congress, leaving the tax credit to expire on December 31.

Source: http://www.wisinfo.com/postcrescent/news/archive/local_15749_685.shtml

[\[Return to top\]](#)

Chemical Sector

3. *April 19, Post Crescent (Appleton, WI)* — **Rural homes cleared due to chemical leak. A chemical tanker overturned and leaked anhydrous ammonia in a farm field northeast of New Holstein, WI, forcing the evacuation of five or six rural homes Saturday night, April 17.** Calumet County Emergency Management Director Chris Nordeng said residents of the evacuated homes were allowed to return at about 10 p.m., roughly two hours after the tanker overturned and released about 390 gallons of the noxious liquid. The spill occurred in a field between Charlesburg and Tecumseh roads, about three miles from New Holstein, and prompted the evacuation. A farm tractor was towing the tanker while spraying fields when the towing pin sheared, causing the tanker to tip and begin losing liquid through a disconnected hose.

Source: http://www.wisinfo.com/postcrescent/news/archive/local_15745_707.shtml

4. *April 19, The Enterprise (Boston, MA)* — **Ammonia gas leak forces evacuation.** A 40-foot vapor plume of ammonia gas escaped from a pipe outside the North East Refrigerated Terminals on Sunday afternoon, April 18, forcing the evacuation of nearby residents.

Responding firefighters saw the vapor escaping from a pipe outside the building. "It was a substantial release," said Capt. Glenn MacNayr, the incident commander at the scene. Shortly after 1:15 p.m., when the call came in, MacNayr gave an immediate order to evacuate the 35–40 homes inside a one–mile radius of the plant. He also closed Wood Street. **Six technicians from the District 1 Hazmat agency and a technician from American Refrigeration, the firm that maintains the refrigeration system at the plant, entered the building and shut down the compressors of the system at 2:45 p.m. By 3:30 p.m., MacNayr reduced the evacuation zone to a quarter mile, which allowed most residents to return home. He said only two homes were inside the quarter–mile radius.** An employee of a nearby electronics firm was also evacuated.

Source: <http://enterprise.southofboston.com/articles/2004/04/19/news/news/news03.txt>

5. *April 19, WHIO TV (Springfield, OH)* — **Chemical leak forces evacuation at Ohio plant.** Investigators said a sulfur dioxide leak was discovered by an employee in International's Wastewater Treatment facility, which is located behind the plant. Sulfur Dioxide is used to help remove chlorine from water and is a potentially dangerous substance. A Hazmat unit was called to help contain the leak. Two employees who may have been exposed to the chemical were taken to International's infirmary as a precaution.

Source: <http://www.whiotv.com/news/3020208/detail.html>

[\[Return to top\]](#)

Defense Industrial Base Sector

6. *April 19, Government Computer News* — **Defense issues wireless policy. The Department of Defense (DoD) has released its long–awaited wireless policy, making it mandatory for all DoD personnel, contractors and even visitors entering Defense facilities to encrypt unclassified information transmitted wirelessly.** The policy, DoD 8100.2, comes nearly two years after DoD issued a Pentagon wireless policy. The directive views wireless devices, services and technologies that are integrated or connected to Defense networks as part of those networks. Data encryption, at a minimum, must be implemented end–to–end over an assured channel and must be validated against Federal Information Processing Standards requirements under the Cryptographic Module Validation Program. The new law prohibits the use of wireless devices for storing, processing or transmitting classified information without "explicit written approval of the cognizant designated approving authority," Paul Wolfowitz, deputy secretary of Defense, noted in the directive. Furthermore, cellular, PC, radio frequency and infrared wireless devices are not allowed, without written approval, in areas where classified information is discussed, electronically stored, processed or transmitted. **Wolfowitz directed Defense agencies to screen for wireless devices within their organizations by using active electromagnetic sensing to detect and prevent unauthorized access of Defense systems.**

Policy: <http://gcn.com/newspics/dodd81002p.pdf>

Source: http://www.gcn.com/vol1_no1/daily-updates/25626-1.html

[\[Return to top\]](#)

Banking and Finance Sector

7. *April 19, Reuters* — **E-mail spammers target share tips in latest scam. Pumping up highly volatile share prices in small companies with a barrage of bullish e-mails is the latest get-rich-quick scam deployed by e-mail spammers. According to spam-detection specialists ClearSwift, the number of spammed stock tips has risen more than 300 percent between December and March, meaning thousands of bogus investment tips are filling in-boxes daily on a variety of obscure firms listed on bourses around the world.** While stock-related spam ranks well below the torrent of unsolicited offers for sexual aids and pornography, the volume has increased dramatically from six months ago when the phenomenon first caught the attention of security professionals. "The spammers are looking at a new angle to cash in. And it's financial services," said Alyn Hockey, director of research at the UK-based ClearSwift. The stock e-mails are less sophisticated, but with unsuspecting e-mail users continuing to fall prey to a variety of low-level scams daily, spam watchers suspect this scam will rise significantly in the coming months with investor enthusiasm on the rise. Profiling the spammers is a difficult task. **Many can be traced back to countries with lax or no financial disclosure laws such as South America or eastern Europe, said Hockey.**
Source: <http://www.reuters.co.uk/newsArticle.jhtml?type=technologyNews&storyID=4865035§ion=news>

[\[Return to top\]](#)

Transportation Sector

8. *April 19, Associated Press* — **LIRR and Amtrak trains bump at station. A commuter train was struck from behind by an empty Amtrak train as they approached Penn Station on Monday morning, April 19, and at least 130 people suffered minor injuries, authorities said.** The accident delayed other trains for the morning rush hour. Both Amtrak and the Long Island Rail Road (LIRR) characterized the accident as minor. It happened shortly after 7 a.m. at the Manhattan end of the East River Tunnel, at a point where trains switch from one track to another beneath the streets of mid-Manhattan. Dozens of commuters with bruises and bloody cuts were led to ambulances outside Penn Station. Fire Commissioner Nicholas Scoppetta said at least 130 people had minor injuries and some were taken to hospitals. "No one critical, no one serious, all injuries appear to be minor," said David Billig, a Fire Department spokesman. Scoppetta said the Amtrak train rear-ended the LIRR train, which was coming into Manhattan from the Long Island town of Ronkonkoma. Other LIRR trains heading into Penn Station were delayed 15 to 30 minutes, and some trains stopped in Brooklyn. Amtrak spokesman Dan Stessel said the Amtrak train was on its way to Penn Station from a rail yard in Queens to pick up passengers for a trip to Washington.
Source: http://abcnews.go.com/wire/US/ap20040419_623.html
9. *April 19, Reuters* — **Cruise lines commit \$200 M for NY port revamp.** New York Mayor Michael Bloomberg said Monday, April 19, two major cruise lines have signed deals to pay \$200 million in fees for preferential berths in the city's planned renovation of the West Side Terminal. **Norwegian Cruise Lines and Carnival Corporation agreed to pay the city at least \$200 million in port charges through the year 2017 and to bring at least 13 million passengers to New York during that time,** Bloomberg said. The city will spend \$150 million to modernize the Manhattan terminal, which has not been updated since the 1970s. The

terminal will be renamed the New York Cruise Terminal. A new berth on the Brooklyn waterfront is also part of the redevelopment plan, which is aimed squarely at keeping New York a major destination for the growing cruise ship business. **The agreements "represent the cruise industry's confidence in the growth of this market," said Bloomberg, noting the cruise industry accounted for more than 3,300 jobs and almost \$600 million in economic activity this year.**

Source: http://www.forbes.com/business/newswire/2004/04/19/rtr133674_0.html

10. April 19, Associated Press — Government may relax airport security rule. Pittsburgh International could become the nation's first major airport to get the OK to abandon the post-September 11 rule that says only ticketed passengers are allowed past security checkpoints. Federal security officials are considering allowing people once more to say their hellos and goodbyes to friends and loved ones at the gate. Airport officials and western Pennsylvania's congressional delegation have pushed for two years for the change for reasons of money and passenger convenience. What happens here could become a model for other airports. Pittsburgh is a strong candidate for the experiment for two reasons: It has a centralized security checkpoint in one terminal. And it has a full-scale shopping mall that has suffered a drop-off in business because it is reachable only by ticketed passengers. If the change is approved, people without tickets will have to go through security just like passengers. They will be checked with metal detectors and may have to empty their pockets and handbags and take off their shoes.

Source: <http://www.cnn.com/2004/TRAVEL/04/19/airport.security.ap/index.html>

11. April 16, Associated Press — Behavior pattern recognition program under way at Logan. A pilot program using "behavior pattern recognition" is under way at Boston's Logan International Airport, from where two of the planes used by the September 11 hijackers took off. Air marshals, passenger screeners and state police stationed there have undergone special training in things to look for that could indicate a terrorist plot. Israeli officials have employed a version of the technique for years to protect air travelers against terrorists. At Logan, uniformed and undercover security officials watch people as they move through terminals. They look for odd or suspicious behavior: heavy clothes on a hot day, loiterers without luggage, anyone observing security methods. At the security checkpoints, screening supervisors have a score sheet with a list of behaviors on it. If a passenger hits a certain number, a law enforcement officer will be notified to question the person. Air marshals watch the airport crowds as they wait for their flights; they, too, alert the troopers if they see something suspicious. **"They're looking for something outside the normal range of behavior," said Jack Shea, special agent in charge of the federal air marshals in Boston. "What I like about it, it's very basic, it's common sense, it's effective, it works."** Massachusetts State Police Maj. Tom Robbins, who oversees the troopers at Logan, said the program has been a success.

Source: <http://www.cnn.com/2004/TRAVEL/04/16/airline.behavior.ap/index.html>

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

Agriculture Sector

12. *April 19, ITAR–Tass News Agency* — **Cattle hit by foot–and–mouth epidemic in Russia. An emergency regime has been established in six regions of the Amur region in the Russian Far East following an epidemic of foot–and–mouth disease that broke out at a cattle farm in the settlement of Sadovoye.** Veterinary, sanitary services, and the Ministry for emergency situations have enforced a triple sanitary cordon around the Sadovoye settlement. Mobile police patrols prevent access of transport vehicles, grain and dairy product supply to and from the quarantined zone. Regional governor Leonid Korotkov chaired an emergency meeting of the headquarters set up to prevent the epidemic which discussed priority preventive measures, including inspections on roads and disinfections at all neighboring cattle farms. Groups have been created and instructed to slaughter. A total of 87 out of 940 species at the Sadovoye cattle farm have been infected, including 57 animals that have already been slaughtered.
Source: <http://www.itar-tass.com/eng/level2.html?NewsID=710082&PageNum=0>

13. *April 18, Associated Press* — **EU rules on GM food labelling come into force.** European countries start enforcing the world's strictest rules on labelling genetically–modified (GM) foods Sunday, April 18. Foods with biotech ingredients already had labelling requirements in the European Union (EU). **But the new rules are tougher because they will include ingredients like vegetable oils and other highly–refined products, such as soy lecithin, where the genetically–modified DNA or resulting protein is no longer present or undetectable in the final product.** The new threshold level is set at 0.9 percent, down from the current one percent. Traceability rules adopted simultaneously require a paper trail "from the farm to the fork" to deter cheating. In preparation for the law coming into force, "a lot of food companies have reformulated or found other supply chains" to avoid using the labels, said Dominique Taeymans, director of scientific and regulatory affairs at the European food and drink industry lobby, CIAA. Farm groups in the United States, the world's leading producer of genetically–engineered crops, have opposed labelling, arguing it is unnecessary because their products have been proven safe. **In the United States, about 80 percent of the soy crop, half of the canola crop and 40 percent of the corn crop comes from genetically–engineered seeds.**
Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1082320712728_112/?hub=World

14. *April 17, Honolulu Advertiser* — **Banana virus strikes Hawaii. Banana bunchy top virus was reported this week on a large banana farm in Keaau, posing a major new threat to Hawaii's \$8.4 million banana industry. The find on a 200–acre Keaau Banana Plantation marks the first time the virus has been detected in East Hawaii, the state's primary banana growing region.** The virus was found on 13 of 25 fields on the plantation, and experts suspect the virus may have spread through the crops for a year before it was discovered, said Nilton Matayoshi of the state Department of Agriculture. Surveys of the farm's fields found the disease on both the apple banana and the commercially popular Cavendish variety of bananas that consumers are more accustomed to seeing in supermarkets. Cavendish is more vulnerable to the virus than apple banana, and the virus has virtually eliminated farming of Cavendish on Oahu, Matayoshi said. The Hawaii Department of Agriculture attempted to block the spread of

the virus on the Big Island by launching an extensive eradication project in 1999 in North Kona after the virus was discovered there. Agriculture officials established a 10-mile eradication zone and destroyed more than 175,000 banana plants over two years as part of the effort, but the virus was never completely wiped out.

Source: <http://the.honoluluadvertiser.com/article/2004/Apr/17/ln/ln03a.html>

[\[Return to top\]](#)

Food Sector

15. *April 18, Associated Press* — **Mexico to lift restrictions on poultry. Mexico's Agriculture Department on Monday, April 19, plans to lift restrictions on poultry imports from four U.S. states. The decision reopens the door for imports of poultry from North Carolina, Maine, Virginia, and West Virginia – where avian flu had been detected.** Restrictions will remain in place on poultry imports from California, Connecticut, Delaware, Maryland, Pennsylvania, and Texas, the department said in a statement. The outbreak of avian influenza in Gonzales, Texas, in February triggered an embargo against U.S. poultry products by Mexico. On February 24, Mexico's Agriculture Department had announced a ban on imports of live birds, eggs, and poultry products from throughout the United States.

Source: <http://www.stamfordadvocate.com/news/local/state/hc-18195247.apds.m0587.bc-ct--mexiapr18,0,82747.story?coll=hc-headlines-local-wire>

16. *April 17, Associated Press* — **U.S. officials optimistic about ending importers' bans on beef and poultry. The United States is making headway in lifting the bans that some of its leading customers have imposed on U.S. beef and poultry exports because of mad cow and bird diseases, U.S. Department of Agriculture (USDA) officials said Friday, April 16.** Next week, China may announce progress toward reducing restrictions on U.S. beef and poultry, and Mexico will announce that it will open its borders to more U.S. poultry, they said. Officials sounded less optimistic about coming talks with Japanese officials. In a wide-ranging news conference, the officials also said the government's plans to increase testing for mad cow disease are on target. China had banned U.S. beef products after the United States announced in December that a Holstein in Washington state had the disease. China banned poultry imports in February after bird flu was found in Texas and unrelated cases were found in East Coast states. About 50 other nations also have refused to accept U.S. beef and poultry. During next Wednesday's cabinet-level talks of the U.S.-China Joint Commission on Commerce and Trade, China could announce progress toward resuming imports, said J.B. Penn, undersecretary for farm and foreign agricultural services.

Source: <http://newtribune.com/articles/2004/04/17/business/0417040022.txt>

[\[Return to top\]](#)

Water Sector

17. *April 19, Associated Press* — **Supreme Court won't intervene in river fight. The Supreme Court refused Monday, April 19, to intervene in a dispute over the Missouri River, passing up a chance to clarify when the government can order water shifting on the river**

to preserve fishing and recreation. The federal government has faced multiple lawsuits over its management of the 2,400-mile river, which runs through seven states from Montana to Missouri. The suits stem from the government's response to a prolonged 2002 drought. The Supreme Court was asked to use the case to interpret a 1944 flood control law that created a system of dams on the Missouri River. Justices declined, without comment. **An appeals court ruled last year that under the law, reservoirs are to be used to control flooding and maintain downstream navigation, with a lower priority given to recreation, and fish and wildlife.** The losers in that decision were Montana, North Dakota, and South Dakota, which opposed the U.S. Corps of Engineers' release of water from their reservoirs to provide relief for down river barge traffic from Sioux City, Iowa, to St. Louis. Lawyers for the Dakotas and Montana told the justices in court filings that the value of recreation to the economy should not be downplayed.

Source: http://www.dfw.com/mld/dfw/news/breaking_news/8467180.htm?1c

[[Return to top](#)]

Public Health Sector

18. *April 19, Cleveland Plain Dealer* — Breaking through the species firewall. New research may help explain how the infectious proteins implicated in illnesses such as mad cow disease are able to penetrate the natural barriers between species. The study, by Case Western Reserve University researchers, shows it is relatively easy for a protein called a prion to morph into a stealthier strain capable of outwitting the species firewall. All it takes is exposure to a fragment of an abnormal prion protein from a third species, a process called seeding. The new prion strain has the same chemical fingerprint as before, but a different three-dimensional shape. Apparently, the altered profile is what enables the rogue prion to escape recognition and slip past the defenses meant to stop species from swapping illnesses. Scientists have suspected such a process allowed sheep-tainted cow prions to infect humans beginning in England in 1995. But they lacked a molecular model demonstrating how prions might have created new strains, enabling them to jump the species barrier. The Case study provides that, several prion experts say. Along with similar recent research in yeast, it also largely rebuts the long-debated idea that something other than or in addition to a prion – a virus, perhaps – causes the family of mad-cow-like illnesses in animals and humans.

Source: <http://www.cleveland.com/living/plaindealer/index.ssf?/base/living/1082367099162511.xml>

19. *April 19, American Medical News* — Measles cases trigger actions in nine states. Two recent measles outbreaks, both imported from abroad, have tested the agility of the post-September 11 public health infrastructure. In March, an Iowa college student, who had not been vaccinated, became infected with measles while in India. Officials at the Iowa Department of Public Health had already been alerted to an outbreak within the student's tour group, but the student returned early against their advice. He flew from New Delhi via Amsterdam and Detroit and developed measles symptoms upon his return to Cedar Rapids, Iowa. The Michigan Department of Community Health traced passengers linked to the Detroit flight and urged them to get vaccinated if necessary. Iowa public health workers organized special vaccination clinics, quarantined those who may have been exposed, and traced two more cases to the student. In neighboring Nebraska, the health and human services system also

urged residents to check to make sure their shots were up-to-date. In a separate incident, the Centers for Disease Control and Prevention reported nine measles cases among a group of infants adopted from China. The babies had traveled with American families to Alaska, Florida, Maryland, New York, and Washington. Additionally, an unvaccinated adult who was exposed to one of the infected infants traveled to California.

Source: <http://www.ama-assn.org/amednews/2004/04/26/hlsb0426.htm>

20. April 17, United Press International — SARS virus carried by more than civets. Chinese scientists have found the coronavirus that causes Severe Acute Respiratory Syndrome (SARS), believed to be found in civets, was also found in foxes, hedgehews, and cats. The Guangzhou Evening News reported Saturday, April 17, Lin Jinyan, the leader of a SARS control research team, reported at a conference in Guangzhou, China, that civets weren't the only animal to carry the virus. The team had tested thousands of people carrying SARS antibodies in 16 cities in Guangdong Province and found among 994 people working in animal markets, 10.6 percent carried positive antibodies, but only 3.25 percent of those working with civet cats tested positive. The scientists then tested other animals and found foxes, hedgehews, and cats carried the SARS coronavirus. World Health Organization experts said on January 16 SARS or a SARS-like coronavirus was carried in civet cats, which infected people via animal markets, said Xinhua, China's main government-run news agency.

Source: http://washingtontimes.com/upi-breaking/20040417-123936-7571_r.htm

21. April 16, Reuters — New drug-resistant type of Salmonella. Researchers have identified a strain of Salmonella choleraesuis (S. choleraesuis) that is resistant to Rocephin (ceftriaxone), an antibiotic that has been a reliable treatment in the past. The emergence of this strain, say the investigators, could have important public health implications. Over the years, they point out that S. choleraesuis has developed resistance to a variety of antibiotics, especially drugs like Cipro (ciprofloxacin). Until now, however, the microbe had always been sensitive to Rocephin. J.T. Ou, from Chang Gung University in Taoyuan, Taiwan, and colleagues describe a strain of S. choleraesuis that was isolated from a man with a severe blood infection. The organism was found to be resistant to all standard anti-salmonella antibiotics as well as to Rocephin and Cipro. Treatment with Primaxin (imipenem-cilastatin) was unsuccessful and the patient died 7 days after hospital admission. **"The appearance of this resistant S. choleraesuis," the researchers conclude, "is a serious threat to public health. Constant surveillance is needed to prevent its further spread."**

Source: <http://www.reuters.com/newsArticle.jhtml?type=healthNews&storyID=4853180>

[\[Return to top\]](#)

Government Sector

22. April 19, Associated Press — Ridge forms task force to prevent terrorist attacks. With an eye on a large number of symbolic gatherings, Homeland Security Secretary Tom Ridge is forming a new government task force to better coordinate public and private security — and hopefully prevent the next terrorist attack. Beginning with the dedication of the new World War II Memorial in Washington over the Memorial Day weekend, Ridge said high-profile public events this year may be attractive targets for al Qaeda and like-minded terrorist groups. "We are rich with opportunities this year for terrorists to shake our will," Ridge said in a telephone

interview Sunday. "We are going to increase our vigilance," he said later. With the new task force, Homeland Security officials will be joined by representatives from nine Cabinet-level agencies in an effort to improve coordination as the government works to secure critical infrastructure and increase the nation's readiness. Ridge said officials don't have specific intelligence about possible attacks. But based on analysis, the government is paying attention to potential targets. **These include next month's war memorial dedication, the June meeting in Georgia of the Group of Eight industrialized nations, large gatherings nationwide for Fourth of July celebrations, the July Democratic convention in Boston, the August Republican convention in New York and the August Olympics in Athens.**

Source: http://www.newsday.com/news/nationworld/nation/ny-usterr0419_0.659115.story?coll=ny-top-span-headlines

23. *April 19, Federal Computer Week* — **DHS funds control systems.** Focus on protecting the nation's critical infrastructures has led to increasing concern about gaps in industrial control systems that monitor and collect data, such as electric power grids or oil and gas pipelines. **To alleviate that concern, 11 of the 66 small-business research grants awarded two months ago by the Homeland Security Advanced Research Projects Agency dealt with developing new technologies to secure supervisory control and data acquisition (SCADA) systems.** Enhancements will include encryption and secure communication between the application server and remote controls that senses whether the connection is via the Internet, telephone or wireless links. Another benefit will be ensuring that only those with authentication and authorization services will be able to access protected remote facilities, **SCADA systems monitor and control processes and physical functions in the electric, oil, gas, water and chemical manufacturing and utility industries,** to name a few. Such systems can manage and control the generation, transmission and distribution of electrical power or remotely monitor the pressure and flow of gas pipelines.

Source: [http://www.fcw.com/fcw/articles/2004/0419/web-scada-04-19-04 .asp](http://www.fcw.com/fcw/articles/2004/0419/web-scada-04-19-04.asp)

[\[Return to top\]](#)

Emergency Services Sector

Nothing to report.

[\[Return to top\]](#)

Information and Telecommunications Sector

24. *April 19, eSecurity Planet* — **ColdFusion MX DoS vulnerability patched.** Graphics design software specialist Macromedia has rolled out a fix for a denial-of-service vulnerability found in its ColdFusion MX 6.1 product suite. The firm said **the flaw affected all editions of ColdFusion MX 6.1 and all versions of ColdFusion MX 6.1 J2EE. Macromedia tagged the issue as "important" and recommended that users apply the accompanying patch immediately.** ColdFusion MX, formerly known as "Neo," is a key part of Macromedia MX, an integrated collection of tool, server and client technologies developed to function as a single environment. But, security bugs have followed the product around with the latest centering around the way ColdFusion MX handles file uploads. "When file uploads to ColdFusion MX

via an HTML form are started, but are interrupted before they complete – disk space on the server may not be reclaimed when the ColdFusion MX template finishes processing," the company explained.

Source: <http://www.esecurityplanet.com/trends/article.php/3342061>

25. *April 16, CNET News.com* — **Cisco issues another security warning.** Cisco Systems warned customers on Thursday, April 15, of what security experts are calling a "minor security issue" in its IPSec-based VPN 3000 Concentrator. The problem, which is present in both Linux and Microsoft versions of the IPSec client, occurs when customers configure the VPN (virtual private network) concentrator to accept group passwords rather than digital certificates for authentication. Typically, a group password is encrypted when used for authentication. But on VPN 3000 Concentrator clients, the password can be extracted from memory, making it available to anyone using a device with the Cisco software client. **People who have gained knowledge of a group password may use it to hijack connections or gain knowledge of sensitive information when these are used as pre-shared keys during authentication.** Cisco recommends that customers deploy PKI (Public Key Infrastructure) instead of a Group Password based authentication scheme. Additional information is available on the Cisco Website: http://www.cisco.com/warp/public/707/cisco-sn-20040415-grppa_ss.shtml
Source: http://news.com.com/2100-7355_3-5193521.html?tag=nefd.top

26. *April 16, eSecurity Planet* — **Multiple Linux flaws reported.** Security researchers are warning of a **buffer overflow security flaw in the Linux kernel that can be exploited to lead to privilege escalation attacks.** According to an advisory issued by iDEFENSE, the vulnerabilities affect Linux Kernel 2.6.x; Linux Kernel 2.5.x and Linux Kernel 2.4.x. The company found that affected versions of Linux kernel performed no length checking on symbolic links stored on an ISO9660 file system, a problem that allows a malformed CD to perform an arbitrary length overflow in kernel memory. "Symbolic links on ISO9660 file systems are supported by the 'Rock Ridge' extension to the standard format. The vulnerability can be triggered by performing a directory listing on a maliciously constructed ISO file system, or attempting to access a file via a malformed symlink on such a file system. Many distributions allow local users to mount CDs, which makes them potentially vulnerable to local elevation attacks," according to the security alert. Updated Linux kernel versions are available at kernel.org. Separately, **security firm Secunia warned of an information leak and denial-of-service holes in Linux Kernel 2.4.x and 2.6.x.** The information leak problem was discovered with the ext3, XFS, and JFS file system code and can lead to the exposure of data like cryptographic keys to malicious attackers. **Another error was found within the OSS code for SoundBlaster 16 devices that could be used to trigger denial-of-service attacks with odd numbers of output bytes are submitted.**
Source: <http://www.esecurityplanet.com/trends/article.php/3341341>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_NETSKY.P 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), 135 (epmap), 80 (www), 137 (netbios-ns), 2745 (urbisnet), 3127 (mydoom), 1433 (ms-sql-s), 1434 (ms-sql-m), 4899 (radmin), 6129 (dameware) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

[[Return to top](#)]

General Sector

27. April 19, The Press Association (PA) — Ten arrested in fresh terror act raids. Ten people were arrested Monday, April 19, in a series of anti-terror raids, amid reports of a planned attack against the huge shopping centre in Manchester. The operation comes less than a month after eight men were detained during a series of raids across south east England which led to the recovery of 600kg of ammonium nitrate fertiliser, which can be used in bomb making. The targets of today's raids included a flat above a fast food takeaway in Upper Brook Street close to Manchester city centre. Police condoned off an area outside the Dolphins takeaway and officers stood on guard.

Source: <http://news.independent.co.uk/uk/crime/story.jsp?story=512919>

[[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.nipcc.gov>), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, 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) 883-3644

Subscription and Distribution Information Send mail to nipcdailyadmin@mail.nipc.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 info@us-cert.gov or visit their Web page at www.uscert.gov.

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.