



Department of Homeland Security

IAIP Directorate

Daily Open Source Infrastructure Report

for 17 June 2004

Current Nationwide Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)

www.whitehouse.gov/homeland

Daily Overview

- The Modesto Bee reports up to 26,000 Modesto Irrigation District (MID) customers in California lost power for about an hour on Tuesday, and officials are not sure why. (See item [2](#))
- US-CERT has announced Vulnerability Note VU#784540: BGP implementations do not adequately handle malformed BGP OPEN and UPDATE messages. (See item [28](#))
- Wired News reports that according to the FBI, eco-terrorism — acts of violence in protest of harm to animals or to the environment — is the United States' number one terrorism threat from inside its own borders. (See item [34](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *June 16, East Valley Tribune (AZ)* — **Nuclear inspection team sent to Palo Verde.** Part of the emergency system used to shut down the Palo Verde nuclear plant near Wintersburg, AZ, failed to work properly on Monday, June 14, prompting the U.S. Nuclear Regulatory Commission to dispatch a team to Arizona to investigate. The equipment ultimately worked well enough to safely shut down all three reactors at the plant, but "because of some complications associated with the event, we want to take a detailed look at what occurred," said Thomas Gwynn, deputy regional administrator for the commission, which is responsible for nuclear power plant safety.

One of the generators used provide power to the plant failed to come on after a power grid interruption triggered a shutdown Monday. A backup generator was used to shut down the reactor. Palo Verde's three reactors were expected to remain closed for several days.
Source: <http://www.aztrib.com/index.php?sty=23165>

2. *June 16, Modesto Bee (CA)* — **Mystery blackout hits city. Up to 26,000 Modesto Irrigation District (MID) customers in California lost power for about an hour Tuesday, June 15, and MID officials were not sure why. Something knocked out nine of MID's 30 substations, said MID spokesperson Kate Hora. Hora estimated the blackout affected between 21,000 and 26,250 of MID's customers, or about 20 percent to 25 percent.** The amount of electricity in use at the time was normal for this time of year and was in line with what the MID expected, she said. While Hora said officials have not been able to identify the cause of the blackout, she said it was not related to Tuesday's hot temperatures. The two most common causes of power failures are storms and car accidents involving power poles, Hora said. "We're pretty certain that whatever happened was in MID's own system and not something external," Hora said. MID officials are trying to determine the exact sequence of events so they can pinpoint the origin of the failure, but Hora said this will take some time. She said in the past there have been blackouts for which the MID was unable to determine the cause.

Source: <http://www.modbee.com/local/story/8717387p-9593710c.html>

3. *June 15, Associated Press* — **LIPA predicts tight supply of electricity this summer.** Supplies of electricity should be sufficient to keep the air conditioners, swimming pool filters and other gadgets running this summer, but the margin for error will be slim, Long Island Power Authority (LIPA) officials said Tuesday, June 15. The electric company said it expects to have 5,500 megawatts of power available on most summer days, enough to meet a summer peak demand of 4,955 megawatts, LIPA Chairman Richard Kessel said. **On days when temperatures soar into the high 90s, however, peak demand for electricity could approach 5,600 megawatts, which will force the company to scramble for additional sources of power, Kessel said.**

Source: <http://www.newsday.com/news/local/wire/ny-bc-ny--lipoweroutlook0615jun15.0.2497575.story?coll=ny-ap-regional-wire>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[[Return to top](#)]

Defense Industrial Base Sector

4. *June 16, Government Computer News* — **DARPA calls for ideas on advanced communication project.** The Defense Advanced Research Projects Agency (DARPA) recently released two requests for comments for its Next Generation Communications program. The technologies that DARPA is developing under the XG program will provide a mechanism for enabling wireless communications systems to access temporarily unused

radio frequency spectrum without causing interference with systems and users, according to a DARPA release. "This is the next step in defining an XG standard for adaptive spectrum access. The policy language provides the ability to decouple policy and engineering in the radio," said Preston Marshall, DARPA's XG program manager. "Where today's radios are designed to comply with specific spectrum policies and cannot adapt to new regulatory environments, software-defined radios that implement the policy language can readily adapt to policy changes without redesign," Marshall added.

Source: http://www.gcn.com/vol1_no1/daily-updates/26232-1.html

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

Banking and Finance Sector

5. *June 16, Accountancy Age* — **Money laundering failure revealed. Accountants in the United Kingdom have failed to respond to the obligation to report money laundering suspicions, according to the National Criminal Intelligence Service.** Accountants have filed just 100 short form reports each month since the changes in March, in contrast to a 60% increase in submissions across all sectors. The news will cause great concern to the profession, whose members can now be jailed for failure to report. It will also disappoint legislators, who introduced the changes partly to tackle perceived auditor apathy on the issue.

Source: <http://www.accountancyage.com/News/1137397>

6. *June 16, Computerworld Online* — **Seventeen companies form group to fight phishing, spoofing. More than a dozen corporate giants in the retail, telecommunications, financial services, banking and technology industries are joining forces to combat phishing, spoofing and other methods of online identify fraud.** On Wednesday, June 16 the companies will announce the formation of the Trusted Electronic Communications Forum (TECF), a group that will focus on eliminating phishing's threat to e-mail and e-commerce. The forum has a complete listing of the companies taking part in the effort on its Website. A statement on the TECF's Website said the companies are concerned about virtual threats that "have impeded the progress of Internet communications and have damaged the trust between enterprises and its customers. These threats include spoofing, phishing and identity fraud," the TECF said, describing itself as "a cross-industry, cross-geographic consortium dedicated to the standardization of technologies, techniques and best practices in the fight against phishing, spoofing and identity theft." **The group said it also plans to focus on standardizing technologies, techniques and best practices to fight cybercrime.**

Source: <http://www.idg.com.hk/cw/readstory.asp?aid=20040616002>

7. *June 16, Government Computer News* — **Inspector general recommends ways to protect Social Security number. The Social Security Administration (SSA) should cross-verify Social Security numbers (SSN) across government and private databases to identify and fix inaccuracies.** That was one of several recommendations proposed on Tuesday, June 15, to lawmakers to protect the integrity of a person's Social Security number. "Cross-verification can combat and limit the spread of false identification and SSN misuse," said Patrick O'Carroll Jr., acting inspector general for the agency. Because Social Security numbers are considered a national identifier, it is a valuable commodity for lawbreakers, O'Carroll told the House Ways and Means Subcommittee on Social Security. **The numbers are valuable tools for identity**

theft and fraud and for terrorists attempting to enter the United States. The SSA should also provide cross-verification capabilities to employers, giving them access to the same data already available to federal, state and local governments, O'Carroll said.

Source: http://www.gcn.com/vol1_no1/daily-updates/26233-1.html

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

Transportation Sector

8. *June 16, Department of Transportation* — **Highway technologies saving money, making roads last longer.** Federal Highway Administrator Mary E. Peters on June 16 toured the construction site on U.S. Highway 67/167 in North Little Rock, AR, getting a firsthand view of technologies that will save taxpayer dollars and provide for a longer lasting road. **The technologies that include high strength, longer lasting concrete, maintenance-free steel beams and higher visibility road markings, are expected to provide a longer lasting roadway with reduced maintenance costs,** Peters said. For example, special weather-resistant steel used in the new bridges never need to be painted over the 50-year lifespan of the bridge, saving the taxpayer dollars and time, she said. "Transportation moves the American economy," Peters said. "When complete, this project will improve the quality of life for the families who commute to jobs, schools and stores using this route."

Source: <http://www.dot.gov/affairs/fhwa804.htm>

9. *June 16, Transportation Security Administration* — **TSA pledges \$2.2 million to Sea-Tac aviation security efforts.** Rear Adm. David M. Stone, Acting Administrator for the Transportation Security Administration (TSA), on June 16 **announced TSA has signed a contract with the Port of Seattle for \$2.2 million to offset the costs of planning and design work for deploying additional Explosives Detection System (EDS) machines in the lobbies of various terminals at Seattle-Tacoma International Airport (Sea-Tac).** The contract is part of TSA's commitment to improving the interim checked baggage security system at the airport as a new permanent in-line system is built. Sea-Tac may use the funding for the services of contractors to manage the planning and design of interim checked baggage solutions for airport terminals and provide construction support and other services required to facilitate construction. TSA has authorized \$955 million in Letters of Intent (LOIs) to airport authorities for the deployment of permanent checked baggage security systems over the next three years, including \$159 million for Seattle-Tacoma International Airport.

Source: http://www.tsa.gov/public/display?theme=44&content=090005198_00ae423

10. *June 16, GovExec.com* — **FAA says it must hire, train air traffic controllers before retirement wave. The Federal Aviation Administration (FAA) must hire new employees far in advance of an impending retirement wave, agency officials and other witnesses testified Tuesday, June 15.** In the next seven years, the FAA faces a major personnel crisis as those hired in the wake of former President Ronald Reagan's 1981 purge of 12,000 air traffic controllers near retirement. The FAA estimates that nearly half of the controller workforce could retire before fiscal year 2012. Legislators on the House Transportation and Infrastructure Subcommittee on Aviation believe the estimate to be extremely conservative because it is based on the retirement of 24 percent of workers in their first year of eligibility. Witnesses and legislators focused on the problem of years-long training for new employees in relation to the

large number of retirees expected in the next decade. For new hires, the certification process, which includes academic and on-the-job training, takes an average of two to four years, according to testimony from the General Accounting Office.

Source: <http://www.govexec.com/dailyfed/0604/061504e1.htm>

11. *June 16, CNN* — **Registered traveler program to begin testing. The Transportation Security Administration (TSA) said Wednesday, June 16, it will launch an experimental program this month to speed frequent travelers through airport security checkpoints.** Groups representing business travelers have pleaded for relief from lengthy preflight security lines, and the registered traveler program tries to strike a compromise between that goal and addressing safeguards imposed after the September 11 attacks. Frequent travelers who voluntarily submit to background checks will be given registered traveler cards. Travelers will have to give the TSA their fingerprints and a scan of the irises of their eyes. The eye scan is among measures known as biometric identifications. Under the three-month pilot program, registered travelers will still have to go through what is called a primary screening — placing carry-on items on conveyer belts at screening points and stepping through a magnetometer. But the cards will allow them, in most cases, to be exempt from secondary screening involving metal-detecting wands.

Source: <http://www.cnn.com/2004/TRAVEL/06/16/registered.traveler/index.html>

12. *June 16, Associated Press* — **New low-cost carrier takes to the skies. Independence Air, the nation's newest discount airline, welcomed its first paying customers Wednesday, June 16, launching a modest schedule of flights serving five cities out of the airline's base at Washington Dulles International Airport.** Atlanta, Boston, Chicago, Newark, New Jersey, and Raleigh-Durham, North Carolina, are the first cities served by the airline, with one-way fares starting at \$49. New destinations will be added beginning next week, said spokesman Rick DeLisi. **To control costs, the carrier is taking reservations only through its Website and by telephone. Independence hopes to appeal to travelers who are unable to meet advance reservation requirements for other carriers' discount fares.** The first flights departed from gates decorated with blue and white balloons to match the planes' color scheme. A water cannon salute greeted the first outbound Bombardier CRJ planes. Discounters JetBlue, Ted, AirTran and Frontier also serve Dulles, which is about 30 miles west of Washington, while rival Southwest is a major presence at Baltimore/Washington International Airport, about 30 miles northeast of the nation's capital.

Source: <http://www.cnn.com/2004/TRAVEL/06/16/bi.independence.air.ap/index.html>

13. *June 16, Department of Homeland Security* — **Multi-layered approach to cargo security outlined. Deputy Secretary Homeland Security James Loy addressed the National Cargo Security Council Annual Convention concerning a new approach to cargo security.** He said, "I am pleased to report, 16 months after President Bush and Congress created the Department of Homeland Security, we have made significant strides... As part of the Transportation Security Administration's Air Cargo Strategic Plan, we began random inspections of air cargo on flights within, into, and out of the United States, and required foreign all-cargo air carriers to comply with the same security procedures that domestic air carriers must follow. We strengthened security at our borders – welcoming the free flow of trade and travelers, but keeping terrorists out. We unified the inspection process – presenting “one face” at the border – and in doing so, nurtured better morale, improved service, and

shorter delays.” For the text of his remarks see:
<http://www.dhs.gov/dhspublic/display?content=3719>
Source: <http://www.dhs.gov/dhspublic/>

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

Postal and Shipping Sector

14. *June 16, Associated Press* — **Postal Service computer error. Thousands of postal workers will receive overpayments this week due to a computer error, the Postal Service said Wednesday, June 16.** An extra close-out payment was due to about 1,900 employees who transferred from management positions to union bargaining unit jobs in 2002, postal spokesman Gerry McKiernan said. The payments varied, but averaged about \$4,000, he said. However, because of a programming error a computer included the extra payments in the checks of 41,434 workers, McKiernan said. He said those workers are being sent letters urging them not to spend the money and explaining how it should be returned.
Source: http://www.centredaily.com/mld/centredaily/news/nation/89371_22.htm

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

Agriculture Sector

15. *June 16, Agricultural Research Service* — **Rapid test for global fungal threat.** Rusts are fungal disease agents that threaten just about every plant or crop in the world. **The science of detecting rusts became a bit more precise this year, as Agricultural Research Service (ARS) scientists have developed a wheat rust species detection kit that relies on a form of rapid DNA testing.** ARS scientists developed the polymerase chain reaction (PCR) test to identify the species that do the most damage to wheat — stem rust, stripe rust, and two species of leaf rust. The test identifies species by detecting specific DNA sequences in fungal genes. Diagnostic labs will likely use the test to analyze rust samples from around the world. Plans for future tests include all the important rusts affecting other major cereal grain crops, including barley, rye, and oats. **Once the scientists develop kits to more accurately identify individual rust species, they will devise additional tests to identify subspecies and genetic lineages. This will allow labs to track the movement of rusts worldwide and to immediately recognize types of these rust fungi that might be new to the United States.**
Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

16. *June 15, Iowa Ag Connection* — **Aphid attack spurs fears. Aphids attacked a southeastern Iowa soybean field last week , fanning fears of a repeat of last year's statewide yield-depleting infestation.** A Mediapolis farmer was walking his 140-acre soybean field to scout for weeds when he discovered the infestation. When the farmer returned from the field, his pant legs were sticky with honeydew excreted by the pests. Doug Tinnes, a sales agronomist with Syngenta Inc., whose territory covers 30 counties in southeastern Iowa, counted at least 100 aphids per soybean plant in the field, and he found plant growth stunted where pests numbered as many as 250 per plant. In recent years, soybean aphids have appeared in parts of Iowa during the second week of June, but in small numbers, said Marlin Rice , an Iowa State

University (ISU) Extension entomologist. **Last week, other ISU Extension specialists reported finding a few aphids near Decorah and Ames.** Last summer, cool, dry weather in late July and early August brought a statewide outbreak of the pest. Aphid-related yield losses ranged up to 20 bushels per acre, contributing to a smaller-than-expected 2003 soybean harvest, said Palle Pedersen, an ISU Extension agronomist.

Source: <http://www.iowaagconnection.com/story-state.cfm?Id=510&yr=2004>

17. *June 15, Purdue Exponent* — **Animal database to help detect terrorism. A data surveillance system being developed by the Purdue University School of Veterinary Medicine accesses a database of records from 325 Banfield Pet Hospitals in 40 states. The computerized records allow researchers to more quickly track the patterns of animal diseases,** said Larry Glickman, professor of epidemiology. If there is an increase in specific diseases, parasites or even in non-specific signs such as respiratory or gastrointestinal problems, the system can determine if there's anything unusual. The centers are located in all major population centers where one might be concerned about new infectious agents by terrorists, said Glickman. Of the 18 diseases listed as "highest concern as possible bioterrorism agents" by the U.S. Centers for Disease Control and Prevention, 17 are zoonotic, or transferable from animals to humans. For the last six months, researchers with the surveillance project have been going through old records to establish what patterns are normal, which will serve as a basis of comparison for any changes. The ultimate goal is to make the results available on a Website so health departments can see any problems in their areas.

Source: <http://www.purdueexponent.org/interface/bebop/showstory.php?date=2004/06/16§ion=campus&storyid=index>

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

Food Sector

18. *June 14, Food and Drug Administration* — **Salmon recall. Catsmo Artisan Smokehouse, of Wallkill, NY, Monday, June 14, urged consumers not to consume smoked salmon purchased from one specialty deli in Manhattan and one Westchester County specialty deli due to the potential of it being contaminated with *Listeria monocytogenes*.** Catsmo Corp. is voluntarily recalling the products, which were produced at their processing facility in Wallkill, NY. The problem was discovered as a result of routine sampling June 2nd by New York State Department of Agriculture and Markets food inspectors. Production of smoked salmon has been suspended while the company investigates the source of the problem. *Listeria* is a common organism found in nature. It can cause serious complications for pregnant women, including stillbirth. Other problems can manifest in people with compromised immune systems and the elderly. No illnesses have been reported to date with this problem.

Source: http://www.fda.gov/oc/po/firmrecalls/catsmo06_04.html

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

Water Sector

19.

June 16, Daily News Tribune (MA) — **Failed water tests prompt inspections. Norwood, MA, officials want to inspect roughly 3,000 homes to search for lead service pipes after the town failed to meet federal water standards for the metal.** The town failed an Environmental Protection Agency (EPA) required test this spring. Norwood is being required to start replacing lead water pipes. The EPA has mandated all communities that failed the test to come up with ways to solve the problem. Those towns will be required to replace seven percent of the lead service pipes each year until it passes the EPA test for two consecutive years. According to test results, more than 10 percent of samples taken exceeded the federal lead threshold of 15 parts per billion. Under the Federal Safe Drinking Water Act, testing is required regularly and samples are taken from at-risk homes, such as those known to have lead pipes. Source: <http://www3.dailynewstranscript.com/localRegional/view.bg?articleid=35500>

20. *June 15, Tri-Valley Herald (CA)* — **Levee break heightens water risks.** The plumbing system of California depends on a delicate network of channels and levees that snake through the Sacramento-San Joaquin Delta. Ten days ago, a levee collapsed, and the system's vulnerabilities were laid bare. The flood inundated the Jones Tract, an 11,000-acre bathtub of an island west of Stockton. The filling of that bathtub created a vacuum effect, sucking saltwater toward the southeastern Delta and forcing authorities to shut down the water pumps that supply 22 million Californians. **Federal and state authorities have known that big waves or an earthquake could cause a much bigger chain reaction of levee failures across the Delta. In such a scenario, multiple islands would be inundated, and saltwater would rush inland, possibly forcing officials to shut down the state and federal water pumps for months, leaving some urban areas dry.** Covering 700,000 acres, the Delta is the West Coast's largest estuary, a breeding ground for fish and fowl and a spigot that provides water to two-thirds of California. Over two centuries, this once-vast expanse of marsh has been channeled and leveed. Since 1971, there have been 43 levee breaches, according to records kept by the state Department of Water Resources. Source: <http://www.trivalleyherald.com/Stories/0,1413,86~10669~22138,37.00.html>

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

Public Health Sector

21. *June 16, South Florida Business Journal* — **Potential bioweapon vaccine. A Miami, FL-based biopharmaceutical company said it and its academic development partner Thomas Jefferson University have entered a cooperative research and development agreement with the U.S. Army's Medical Research Institute of Infectious Diseases. The agreement is to advance the development of the company's vaccine for botulinum toxin.** The major goal, the company said, is to develop a safe and effective botulinum toxin vaccine for mucosal — oral or nasal — delivery. The company described botulinum neurotoxin as the most poisonous natural toxin known. Currently, the company said, the only way to prevent botulinum poisoning is immunization with an antiquated, experimental vaccine available in limited supply from the U.S. Centers for Disease Control and Prevention. **"Botulinum toxin is considered a serious threat as a weapon and as an agent of bioterror, due to its lethality in small doses and ease of manufacture,"** the company said, adding several nations, including the former Soviet Union and Iraq, developed and stockpiled bioweapons containing botulinum toxin.

Source: <http://southflorida.bizjournals.com/southflorida/stories/2004/06/14/daily26.html>

22. *June 16, Associated Press* — **Hospital patients possibly exposed to HIV. A Long Island, NY, hospital notified 177 patients that they may have been exposed to HIV or hepatitis because equipment used to check their digestive systems might not have been properly cleaned.** North Shore University Hospital spokesman Terry Lynam said doctors believed the risk of transmission was minuscule and that the letters were a precautionary measure. **Of the 177 people sent letters last week, 86 have already undergone tests and none have tested positive for either virus, the hospital said. All of them are supposed to be retested in six months.** The hospital said it did not have records that medical instruments used for upper endoscopies or colonoscopies were properly disinfected for procedures performed from April 28 to May 10. Workers apparently failed to test disinfectant levels in the water used in a cleaning machine, the hospital said. One of the workers was fired and a second has been suspended without pay, it said.

Source: <http://msnbc.msn.com/id/5224065/>

23. *June 16, Associated Press* — **Botswana finds first polio case in years. The discovery of Botswana's first polio case in 13 years is a wake-up call to other African countries believed to be free of the crippling disease, UN officials warned amid a massive door-to-door immunization campaign. Botswana is the ninth previously polio-free country on the continent to become re-infected following an outbreak in West and Central Africa.** A young boy from the northern town of Maun was reported infected on February 8 with a strain of the disease traced to Nigeria, some 1,550 miles north of this southern African nation. Nigeria's northern state of Kano has been the global epicenter of polio since last October, when authorities there kept children from being inoculated because of persistent rumors the vaccines are unsafe. Fears that health officials could meet similar resistance in Botswana led the government to obtain a High Court order last week making it illegal for parents to refuse to have their children vaccinated. Officials at the UN Children's Fund and World Health Organization warned that the disease spreads rapidly and say just one case can expose up to 100,000 people to infection. Polio usually infects children under five through contaminated drinking water and attacks the central nervous system, causing paralysis, muscular atrophy, deformation, and, in some cases, death.

Source: <http://www.macon.com/mld/macon/news/world/8937173.htm>

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

Government Sector

24. *June 16, Government Technology* — **Miami-Dade county launches local homeland security Website.** County Manager George M. Burgess announced the launch of the first-ever Miami-Dade homeland security Website during a media briefing on June 7. **The Website will enhance Miami-Dade County's efforts to keep residents informed about the threat of terrorism and other disasters.** It will provide comprehensive information including how to prepare a disaster plan and kit, the latest news on homeland security and links to other important and informative Websites. When needed, "Protective Measures" will also be posted at the site to further reduce vulnerability or increase response capability during a period of heightened alert. Burgess also announced the appointment of Michael J. Crisler as Miami

Dade's Public Safety Program Manager. Crisler will serve as coordinator for information technology initiatives across all public safety departments. In addition, he will be a technical advisor to executive staff in the area of cyber security, critical infrastructure protection and privacy. Crisler will take a lead role in developing a countywide IT security awareness program.

Source: <http://www.govtech.net/news/news.php?id=90565>

25. *June 16, CongressDaily* — **Senate panel passes homeland security spending bill. The Senate Homeland Security Appropriations Subcommittee approved its fiscal 2005 spending bill Wednesday, June 16, marking the first Senate action on appropriations bills.** The subcommittee, operating under tentative 302(b) allocations, approved \$33.1 billion for the Homeland Security Department — \$896 million more than President Bush requested. Yet Democrats on the panel argued more funding is needed to bolster homeland security. The Senate bill contains \$5.2 billion for the Transportation Security Administration — \$2 billion more than the House bill. It appropriated \$7.4 billion for the Coast Guard, while the House allocated \$6 billion. The Senate bill contains the same amount — \$340 million — for the transportation agency's new system to track foreign visitors entering and exiting the country. Source: <http://www.govexec.com/dailyfed/0604/061604cdpm2.htm>

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

Emergency Services Sector

26. *June 16, WSTM TV (NY)* — **County emergency drill no small matter. In Syracuse, NY, Tuesday, June 15, emergency preparedness officials were up against one of the most feared bioterrorism agents: small pox. Law enforcement and emergency personnel were being drilled as part of an evaluation of how prepared Central New York is to reacting to a bioterrorist attack.** Inside the Onondaga County Emergency Management Center, a tense situation developed, as the FBI, state and local police, and over a dozen emergency personnel worked the phones, pin pointing vaccination sites and trying to work through what could have been a real life bio terrorist attack. "In these times, after 9/11, communities of every size need to respond to any kind of emergency, whether it's a natural disaster or man made, or some type of bioterrorism," said County Executive Nick Pirro. **"Small pox is one of the most likely and feared, and it's one of the ones that the CDC has concentrated on," said Health Commissioner Dr. Lloyd Novick.** The drill's purpose was designed to test and improve the vaccination process of first responders. Inside the Syracuse Boys and Girls Club, police, fire and emergency personnel got vaccinated. Instead of needles and vaccines, cue tips and water were used. The drill took organizers months to plan, and the OEM says they have more scenarios in the works, including a large-scale water front disaster drill.

Source: <http://www.wstm.com/Global/story.asp?S=1943815&nav=2aKDNxn5>

27. *June 16, KAIT TV (Jonesboro, AR)* — **Mock disaster drill keeps emergency agencies on alert. Since September 11th, the treat of terrorist attacks has become very real, and some say that being prepared is the key to survival...and 13 counties in Northeast Arkansas agree.** June 16, Wednesday's mock disaster drill looked like a scene from a movie: Bodies on the ground, men in white 'space suits,' and emergency personnel saving lives. Gary McCracken, a Registered Nurse at St. Bernard's said, "With terrorism on the rise as it is, and the concerns all

over the country, it's important that we know how to handle that." "This is probably the largest drill that we've ever participated in. this was the whole region, all the way from Helena from the south up to Piggott in the north and all the acute care hospitals and counties involved have been involved in planning this," said Kathryn Blackman, Regional Leader of the NEA Bio-Terrorism. It's also a way for emergency and medical officials to brush up on their crisis skills. Fire Chief Butch Herring said, "It's very important for us to be able to stay in tune and work with other area agencies this gives everyone an opportunity to come together."

Source: <http://www.kait8.com/Global/story.asp?S=1947192>

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

Information Technology and Telecommunications Sector

28. *June 16, US-CERT* — Vulnerability Note VU#784540: BGP implementations do not adequately handle malformed BGP OPEN and UPDATE messages. Multiple BGP implementations contain vulnerabilities handling exceptional OPEN and UPDATE messages. **While the details of the individual vulnerabilities are different, the impacts appear to be limited to denial of service.** In addition, most BGP implementations do not accept messages from arbitrary sources. Some BGP implementations only accept TCP connections (179/tcp) from properly configured peers, and some implementations require a valid AS number in the BGP message data. To deliver malicious messages to such systems, an attacker would need to spoof a TCP connection or have access to a trusted BGP peer. The attacker may also need to know a valid AS number. A remote attacker can cause a denial of service in a vulnerable system. In most cases, the attacker would need to act as a valid BGP peer. BGP session instability can result in "flapping" and other routing problems that may adversely affect Internet traffic. **US-CERT recommends that users apply a patch or upgrade as specified by your vendor.**

Source: <http://www.kb.cert.org/vuls/id/784540>

29. *June 16, Government Technology* — California issues electronic voting machine standards. California Secretary of State Kevin Shelley Tuesday, June 16, adopted state standards for an Accessible Voter Verified Paper Audit Trail (AVVPAT) for electronic voting systems. In doing so, California becomes the first state in the nation to establish requirements for the development and testing of paper audit trails for electronic voting machines. On April 30, Shelley announced that no county or city may purchase a new direct recording electronic (DRE) voting system that does not include an AVVPAT. Currently, July 1, 2006, is the date that all electronic voting systems used in California, regardless of when they were purchased, must have a paper trail. However, the Legislature is now considering moving up that date to January 1, 2006, in order to accommodate the Primary Election. **The standards establish minimum levels of performance for the components required, and establish requirements to ensure privacy, readability, and accessibility.** The requirements are outcome-based, ensuring that manufacturers meet basic requirements without stifling innovation. Conformance to these standards is required for a system to be certified for use in state elections. One key component of the standards is that **the paper copy of each vote must be displayed securely under plastic or glass so that voters can see how they voted, but cannot physically handle the paper.** **This guarantees that each electronic vote has a corresponding paper record that is available in the event of a recount.**

Source: <http://www.govtech.net/news/news.php?id=90568>

30. *June 16, Washington Post* — **Comcast technical glitch causes malfunction.** On Monday night between about 8:30 and 11:30, many of Comcast Corporation's digital-cable subscribers in Washington, DC, were shown nothing but the Disney Channel on all of the company's channels. In the event of an emergency, every cable company has assigned one of its channels to broadcast the government's emergency alert signal, which would instruct viewers as to the nature of the situation and what they should do. In Washington, Comcast picked the Disney Channel for its central location on the lineup, its wide bandwidth and its strong signal to ensure the alert would be widely seen, said Mitchell Schmale, a Comcast spokesman. **On Monday night, a piece of equipment regulating the emergency system malfunctioned. It switched Washington digital-cable subscribers over to the Disney Channel.** When the emergency system is activated, viewers' remote controls are disabled.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A44638-2004Jun 15.html>

31. *June 16, CNET News.com* — **Feds: VoIP a potential haven for terrorists.** The U.S. Department of Justice on Wednesday, June 16, lashed out at phone calls carried across the Internet, saying the fast-growing technology could foster "drug trafficking, organized crime and terrorism." Laura Parsky, a deputy assistant attorney general in the Justice Department, told a Senate panel that law enforcement bodies are deeply worried about their ability to wiretap conversations that use voice over Internet Protocol (VoIP) services. Police been able to conduct Internet wiretaps for at least a decade, and the FBI's controversial Carnivore (also called DCS1000) system was designed to facilitate online surveillance. But Parsky said that **discerning "what the specific (VoIP) protocols are and how law enforcement can extract just the specific information" are difficult problems that could be solved by Congress requiring all VoIP providers to build in backdoors for police surveillance.** Wednesday's hearing was the first to focus on a bill called the VoIP Regulatory Freedom Act which would ban state governments from regulating or taxing VoIP connections. One of the Justice Department's objections to the bill is that it does not impose wiretapping requirements on Internet-only VoIP networks that do not touch the existing phone network. **The Senate's action comes as the FCC considers a request submitted in March by the FBI. If the request is approved, all broadband Internet providers will be required to rewire their networks to support easy wiretapping by police.**

Source: http://news.com.com/Feds%3A+VoIP+a+potential+haven+for+terrorists/2100-1028_3-5236233.html?tag=nfd.top

32. *June 15, eWEEK* — **FTC shoots down spam registry, boosts authentication scheme.** The Federal Trade Commission (FTC) on Tuesday, June 16, told Congress that a proposed National Do Not E-mail registry was unworkable until a universal e-mail authentication standard was adopted. However, this technological step may in turn make such a registry unnecessary. The announcement should give another boost to fast-moving initiatives to better authenticate senders of e-mail by improving SMTP, the transport protocol used by e-mail servers. Such authentication would eliminate most spam, say its proponents. The FTC in its report to Congress said that it would sponsor an Authentication Summit in the fall "to encourage a thorough analysis of possible authentication systems and their swift deployment." The Commission was responding to the December 2003, Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) which called for the FTC to develop a plan

and timetable for establishing a National Do Not E-mail Registry. **The FTC said it studied three possible registries: a registry containing individual e-mail addresses; a registry containing the names of domains that did not wish to receive spam; and a registry of individual names that requires all unsolicited commercial e-mail to be sent via an independent third party that would deliver messages only to those e-mail addresses not on the registry.**

Source: <http://www.eweek.com/article2/0.1759.1612900.00.asp>

33. June 15, PC World — Your PC may be a haven for spies. According to a report being released this week by EarthLink and security software vendor Webroot, as many as one out of three PCs could contain spyware that can secretly record and transmit sensitive personal information. Those figures come from EarthLink's SpyAudit, a Web-based service that helps users discover whether their systems harbor spyware. Since going online in January, **SpyAudit has performed 1.5 million audits and uncovered more than 500,000 copies of Trojan horses and secret monitoring software on users' hard drives.** Matt Cobb, vice president of core operations for EarthLink, cautions that the audit figures don't necessarily mean that one of every three computers is compromised. Some machines may contain more than one copy of malware, and the same machines may have undergone several audits, boosting the overall totals. **From January through April, SpyAudit also detected more than 7 million copies of adware programs—software that delivers browser pop-up ads—and another 32 million instances of adware-related cookie files.**

Source: <http://www.pcworld.com/news/article/0.aid.116526.00.asp>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis	
<p>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.</p>	
<p>Watch Synopsis: Internet scans for backdoor and Trojan Horse ports continue to top the lists of all reporting organizations. The likely reason for such scans are that Bot Networks continue to amass zombie hosts from prior infected hosts such as Sasser and Bagel victims. The use of "botnets" to create denial of service attacks remain a serious threat to the National Infrastructure.</p>	
Current Port Attacks	
Top 10 Target Ports	<p>80 (www), 1026 (nterm), 1080 (socks), 9898 (dabber), 3128 (squid-http), 1025 (blackjack), 1434 (ms-sql-m), 5554 (sasser-ftp), 135 (epmap), 1027 (icq)</p> <p>Source: http://isc.incidents.org/top10.html; Internet Storm Center</p>
<p>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.</p>	
<p>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/.</p>	

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

General Sector

34. *June 16, Wired News* — **Eco-terror cited as top threat. The FBI says eco-terrorism -- acts of violence in protest of harm to animals or to the environment -- is the United States' number one terrorism threat from inside its own borders.** In the early 1990s, biotech executives and scientists were inundated by harassment and violence in Europe. In 1996, the violence began spreading to the U.S. when demonstrators burned a Forest Service truck in the Willamette National Forest in Oregon. In August 2003, two pipe bombs exploded at a pharmaceutical company in Emeryville, CA, followed by another explosion in September 2003 at a health and beauty products company in Pleasanton, CA. **The FBI estimates that domestic eco-terrorism has caused \$110 million in property damage since 1976.** Gary Perlstein, a professor of criminal justice at Portland State University, points out that the figure excludes lost research, increased security costs, lost productivity, and abandoned grants. **About 1,100 criminal acts have been committed in the name of animals or the environment since 1976, the FBI says.** The Earth Liberation Front claimed responsibility for an August 2003 arson in which condominiums being built in California burned to the ground, causing up to \$50 million in damage. Other incidents over the past decade include torching SUVs and other intentional fires at university tree research sites, logging sites, and fast-food restaurants.

Source: http://www.wired.com/news/medtech/0,1286.63812.00.html?tw=wn_tophead_3

35. *June 15, Associated Press* — **Weapons seized in Paris terror raids. French anti-terror police arrested 13 people, including a Muslim prayer leader, and seized weapons in raids Tuesday, June 15, of suspected Islamic militants in the Paris region, police said.** Police said the suspects were thought to have been involved in forging official papers. Blank documents and plastic laminating materials were found in the sweep. The suspects, aged 25 to 35, were detained in connection with a judicial investigation opened last week, the officials said without elaborating. They all reportedly were from the Salafist movement, which holds to a strict interpretation of Islam. **In Spain, authorities also announced progress with anti-terror probes. Judge Baltasar Garzon said he has completed his investigation of an alleged al Qaeda cell accused of helping plan the September 11, 2001, attacks in the United States.** He did not disclose his findings, but completing the probe could possibly set the stage for a trial. Garzon has indicted 40 people on terrorism charges, including 10 he accused specifically of helping plan the September 11 attacks.

Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1087295415144&call_pageid=968332188492&col=968705899037

[[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.