Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 26 April 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Los Angeles Times reports concerns over illegal immigration are spreading, with grass−roots organizations forming to pass initiatives and pressure politicians into enacting laws denying benefits to illegal immigrants. (See item 6)
- The Washington Post reports a drop in the bird flu virus mortality rate portends a new danger, indicating that the bird flu outbreak in Southeast Asia is taking an ominous turn toward a possible global pandemic. (See item 15)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; 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: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact 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 25, Associated Press* — **Valero Energy agrees to buy rival.** Valero Energy Corp. plans to acquire Premcor Inc. for $6.9 billion in cash and stock as part of a deal that would create the largest refiner of crude oil in North America, company officials announced Monday, April 25. With the proposed acquisition, Valero will have total assets of $25 billion and annual revenues of nearly $70 billion, which would rank it No. 15 on the current listing of the Fortune 500. Adding Premcor's refineries in Port Arthur, TX, Memphis, TN, Delaware City, DE, and Lima, OH, will give San Antonio, TX−based Valero 19 refineries with a total throughput capacity of 3.3 million barrels per day. The boards of directors of both companies unanimously approved the acquisition, which is subject to the approval of Premcor's shareholders and customary

regulatory approvals. The transaction is expected to close December 31.
Source: http://www.nytimes.com/aponline/business/AP−Oil−Refinery−Mer ger.html

2. *April 25, Associated Press* — **Spring snowstorm causes power outage in Midwest.** An unusual spring storm dumped nearly two feet of wet snow on parts of the Midwest and Appalachians. The two−day weekend storm brought temperatures as much as 25 degrees below the normal of around 60 as snow fell across parts of Michigan, Indiana, Ohio and western Pennsylvania, and south along the Appalachians as far as western North Carolina. Snapped branches and power lines left about 80,000 FirstEnergy customers in the Cleveland, OH, area without power Sunday, April 24. About 54,000 customers were still without power Monday, April 25, the utility said.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/nation/3151189

3. *April 22, The Midwest Independent Transmission System Operator, PJM Interconnection, and the Tennessee Valley Authority* — **Multi−regional energy pact signed.** The Midwest Independent Transmission System Operator, Inc. (Midwest ISO), PJM Interconnection (PJM) and the Tennessee Valley Authority (TVA) have signed a Joint Reliability Coordination Agreement (JRCA) that will provide for cooperation in the management and operation of the electric transmission grid over a major portion of the eastern United States. The JRCA will result in actively managing the reliability of seams between the wholesale electricity markets of the Midwest ISO and PJM and the service territory of TVA. It provides for the comprehensive management of reliability and relief of congestion within the three power systems. To accomplish this, the parties will share critical operating information, system models and extensive planning data to ensure that all have the best information possible in their daily operations. This information sharing will enable each transmission provider to recognize and manage the effects of its operations on the adjoining systems. The three organizations have also agreed to conduct joint planning sessions to ensure that improvements to their integrated systems are undertaken in a cost−effective manner and without adversely affecting reliability to any organization's customers.
Source: http://www.pjm.com/contributions/news−releases/2005/20050422 −miso−pjm−tva.pdf

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *April 23, Associated Press* — **Chlorine leak forces evacuation.** About 20 homes in a private residential community and an office complex in Hilton Head, SC, were evacuated Friday, April 22, as a precaution after a chlorine cylinder at a public service plant began leaking, officials said. A Hilton Head Plantation resident smelled chlorine that had leaked from the water−cleaning system and called authorities, said Peter Kristian, the community's general manager. The tank was leaking from the bottom as a result of corrosion over time, said Joheida Fister, a spokesperson for Hilton Head Island Fire and Rescue. She was unsure of how much chlorine gas leaked from the cylinder. There were no reported injuries, and the leak was stopped by early afternoon
Source: http://www.thestate.com/mld/thestate/news/local/11464761.htm

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *April 25, Dayton Business Journal* — **Identity theft costs small business.** Small businesses aren't immune from the data security breaches that have recently stung LexisNexis Corp. and DSW Corp., experts say. They said small business owners are faced with myriad issues involving data security. Companies of every size must guard their databases against intruders and in case of a breach, notify customers and salvage their businesses reputation. Despite the high−profile cases at large corporations, small business networks are particularly vulnerable to attack, said Vincent Weafer, senior director of security response for Symantec, an Internet security company. Local offices of large corporations are subject to attacks from hackers who see them as a weak entry point to the entire corporation's network, Weafer said. Also, small businesses tend to overprotect one computer, for instance one that houses the accounting software, but leave others unprotected. Intruders will use the unprotected computers as a way to get into the better−protected machine, Weafer said. Spammers also are attracted to small business computer networks because they tend to be left on, allowing the spammer to constantly send e−mails, he said.
   Source: http://www.bizjournals.com/dayton/stories/2005/04/25/story6.html?GP=OTC−MJ1752087487

[Return to top]

Transportation and Border Security Sector

6. *April 25, Los Angeles Times (CA)* — **Illegal immigration concerns spread.** The armed volunteers patrolling the Arizona−Mexico border may be the starkest sign of frustration with the nation's immigration laws, but across the country there is a growing populist movement also taking matters into its own hands. In Washington, Colorado, Virginia, and elsewhere, grass−roots organizations are forming to pass initiatives and pressure politicians into enacting laws denying benefits to illegal immigrants. There are already groups in seven states and more are expected by the end of summer. Such efforts in places so far from the southern border are testimony to the growing reach of immigration. "Immigration is now a national phenomenon in a way that was less true a decade ago," said Mark Krikorian, executive director of the nonpartisan Center for Immigration Studies in Washington. Supporters of tougher enforcement say the rise of citizen groups is a natural response to the federal government's reluctance to repair a situation nearly everyone admits is broken. The real inspiration has come from Kathy McKee, who launched Proposition 200, which passed overwhelmingly last year in Arizona. The measure requires evidence of legal residence before people can vote or get state welfare services.
   Source: http://www.latimes.com/news/nationworld/nation/la−na−grassroots25apr25,0,7960156.story?coll=la−home−headlines

7. *April 25, Clarksburg Exponent Telegram (WV)* — **Chemical trucks heavily regulated.** While accidents exposing hazardous materials are not common on West Virginia's highways, federal regulations are set up for prevention, yet also to track and contain incidents when they do occur. For example, individuals and trucking companies are required to train and follow federal procedures, said Joe Delcambre, a spokesperson for the Pipeline and Hazardous Materials Safety Administration, a division of the U.S. Department of Transportation. When an incident occurs involving a hazardous material, drivers or their companies are required to report the incident to the Department of Transportation, Delcambre said. Hazmat training can be done in two ways: Industry associations, like the American Trucking Association, train drivers. And Delcambre's agency trains companies and individuals at a site in Oklahoma City. Also, under new permitting regulations, if a trucker is driving north from Beckley to Wheeling, WV, dispatchers need to know the route he's traveling and the cargo he's carrying, according to Bill MacLeod, a spokesperson for the Federal Motor Carriers Safety Administration, another U.S. Department of Transportation agency. Regular radio contact is also important, he said.
Source: http://www.cpubco.com/cgi−bin/LiveIQue.acgi$rec=19119cbgCurrentLocalNews?cbgCurrentLocalNews

8. *April 25, CNN* — **Search for Japan train crash survivors.** Emergency crews in Japan are continuing to search for people trapped in the wreckage of a commuter train that left the tracks and slammed into an apartment building. At least 57 people were killed Monday and 440 others were injured in the country's worst train crash in four decades. Fire department officials said at least four people traveling in the front car of the commuter train were believed to be alive in the wreckage. The seven−car train carrying 580 passengers derailed in an urban area near Osaka in central Japan −− about 255 miles west of Tokyo. Train operator Japan Rail West said at least 343 people had been taken to hospitals. Police and fire officials said they feared the death toll would rise. The train hit several vehicles before hitting the nine−story apartment complex just six meters (20 feet) from the tracks. Five cars derailed, and one car was left wrapped around the building's first−floor car park. Railway officials are checking the train's automatic braking system to see if it was operating properly. Kyodo News reported the system at that stretch of track is among the oldest in Japan.
Source: http://www.cnn.com/2005/WORLD/asiapcf/04/25/japan.rail.crash /index.html

9. *April 25, CNN* — **TSA to test new security technology.** Clam diggers on the muddy flats near Boston's Logan International Airport in Massachusetts will be loaned GPS−equipped cell phones so they can alert authorities to suspicious activity −− just one of several ideas being tested this summer to protect airports from terrorists. Five international airports will test new technology ranging from the cell phones to high−tech iris scanners, the Transportation Security Administration announced Monday, April 25. The airports taking part in the pilot programs are Logan in Boston, JFK International Airport in New York, Denver International Airport in Colorado, Orlando International Airport in Florida and Utah's Salt Lake City International Airport. The new tests constitute phase two of a plan to improve security around airport perimeters, which are of particular concern because of people could position themselves outside airports with shoulder−fired missiles, known as man−portable air defense systems (MANPADS). At Logan, the TSA and the Massachusetts Port Authority also will test an advanced water perimeter intrusion detection system, said retired Rear Adm. David M. Stone, assistant secretary of homeland security for the TSA. The new system includes an infrared

intrusion detection system that will identify authorized people near active runways.
Source: http://edition.cnn.com/2005/TRAVEL/04/25/airport.security/

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

10. *April 24, Florida Today* — **Parasite infected shrimp appearing in lagoon.** Shrimpers in Titusville and Melbourne, FL, report netting more pink shrimp infected with a parasite that causes cotton−like growths. Biologists have yet to determine the prevalence of the parasite or its implications for the Indian River Lagoon. The condition, also called "milk" shrimp, weakens or paralyzes the shrimp, making them unable to reproduce or escape predators. The parasite binds to, destroys, and replaces the shrimp's flesh. State wildlife biologists began getting calls in early February about pink shrimp with the strange growths, mostly in the northern Indian River and Mosquito lagoons. Usually, about one percent to five percent of the lagoon's pink shrimp have the disease, but state biologists say the shrimpers' reports suggest as many as five percent to 20 percent may be infected. The parasite is a single−celled organism called Agmasoma duorara that spends part of its life cycle in fish. Shrimp catch it when they eat other infected marine life. They can contract it from any crustaceans or decaying fish tissue they eat or come in contact with, biologists say. The disease changes the shrimp meat's texture and taste, making them unmarketable.
Source: http://www.floridatoday.com/apps/pbcs.dll/article?AID=/20050424/NEWS01/504240329/1006

11. *April 24, Associated Press* — **White dogwoods threatened.** A disease that is slowly killing off white dogwoods has affected more than half of the trees in Mammoth Cave National Park. The fungus has affected about 70 percent of the 82−square−mile national park in south−central Kentucky, park officials said. Of the 2,298 trees selected at random and examined by park officials, 43 percent had been partially affected by the fungus called dogwood anthracnose, 28 percent had been killed by the disease, and 29 percent were healthy, park officials said. William Jones, a plant pathologist with the U.S. Forest Service, said the disease probably came from an unknown foreign country. In the last decade, the East has lost about half of its native dogwoods. In the late 1980s, there were 807 million dogwoods. Now, there are about 505 million, according to estimates from the Forest Service.
Source: http://www.kentucky.com/mld/kentucky/news/local/11475098.htm

12. *April 22, Wired* — **Cave farming boosts crop yields.** Purdue researchers and entrepreneur Doug Ausenbaugh didn't launch an underground farm because they thought it would yield more crops. They wanted to provide biotech companies a safe environment for growing crops containing pharmaceutical drugs for humans. But they were pleasantly surprised to find that not only did the former quarry apparently keep pollen from the corn, tobacco, soybeans, tomatoes,

and potatoes from escaping, but it also led to higher yields than greenhouses or outdoor fields. The average yield for the genetically modified corn (Bt corn, which contains a gene that produces a protein that kills larvae of the European corn borer) grown in the facility was 337 bushels per acre. The researchers also grew corn in a greenhouse, getting 267 bushels per acre. The average yield for field corn in the U.S. is just 142 bushels per acre. The researchers say they can achieve higher yields in the cave thanks to the controlled environment. Although it's more expensive to grow crops in an artificial environment, higher yields could help offset the cost. Mitchell says that if they can make the lighting system even more efficient, the cave system could revolutionize U.S. farming, whether it involves growing genetically modified or conventional crops.
Source: http://www.wired.com/news/medtech/0%2C1286%2C67305%2C00.html ?tw=wn_2techhead

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

13. *April 25, Associated Press* — **IBM to test health care data sharing.** Hoping to prove that automation will improve health care and cut costs, International Business Machines Corp. (IBM) said Monday, April 25, it's developing a test system for sharing electronic medical data among hospitals, agencies, and patients. The Interoperable Health Information Infrastructure test project, which is expected to be operational by year−end, will connect IBM sites in San Jose, CA, Rochester, MN, and Haifa, Israel. Researchers will use a variety of real and doctored data. It's estimated a move to electronic medical records could shave 10 percent or more from the $1.7 trillion spent on health care each year in the U.S. alone. Besides possibly lowering costs, an interoperable system would help improve the quality of health care by enabling instant access to records anywhere and minimizing the potential for mistakes. A comprehensive, global system also could be used to quickly identify biological attacks and emerging epidemics. Some of the data used in the test system will attempt to mirror such scenarios, said James Kaufman, research manager at IBM.
Source: http://www.nytimes.com/aponline/technology/AP−IBM−Health−Dat a.html?

14. *April 24, Nature Medicine* — **Development of a humanized monoclonal antibody with therapeutic potential against West Nile virus.** Neutralization of West Nile virus (WNV) in vivo correlates with the development of an antibody response against the viral envelope (E) protein. Using random mutagenesis and yeast surface display, researchers defined individual

contact residues of 14 newly generated monoclonal antibodies against domain III of the WNV E protein. Monoclonal antibodies that strongly neutralized WNV localized to a surface patch on the lateral face of domain III. Convalescent antibodies from individuals who had recovered from WNV infection also detected this epitope. One monoclonal antibody, E16, neutralized 10 different strains in vitro, and showed therapeutic efficacy in mice, even when administered as a single dose five days after infection. A humanized version of E16 was generated that retained antigen specificity, avidity and neutralizing activity. In postexposure therapeutic trials in mice, a single dose of humanized E16 protected mice against WNV−induced mortality, and may therefore be a viable treatment option against WNV infection in humans.
Source: http://www.nature.com/nm/journal/vaop/ncurrent/abs/nm1240.ht ml

15. *April 23, Washington Post* — **Drop in bird flu virus mortality rate portends new danger.** More than a year after avian influenza emerged in East Asia, killing more than two−thirds of the people with confirmed cases, Vietnamese doctors are reporting that the mortality rate in their country has dropped substantially. This could mean the outbreak of bird flu in Southeast Asia is taking an ominous turn. If a disease quickly kills almost everyone it infects, it has little chance of spreading very far. The less lethal bird flu becomes the more likely it is to develop into the global pandemic. The mortality rate for bird flu in Vietnam this year is about 35 percent, almost exactly half that of last year, according to Health Ministry statistics. The mortality rate of the 1918 Spanish flu pandemic, by comparison, was less than five percent, but the outbreak killed an estimated 40 million people worldwide. Vietnamese health experts said their suspicion that the disease is shifting is further supported by preliminary research showing a genetic change in the virus in north Vietnam resulting in the production of a protein with one less amino acid than in south Vietnam.
Source: http://www.washingtonpost.com/wp−dyn/articles/A10548−2005Apr 22.html

16. *April 23, Lancet* — **Drug combination offers best treatment option for malaria.** Many countries in Africa are considering a change to combination treatment for falciparum malaria because of the increase in drug resistance. Researchers aimed to study the effectiveness of three drug combinations that have proven efficacious in east Africa. Researchers undertook a random trial of antimalarial drug combinations for children (aged four to 59 months) with uncomplicated malaria in Muheza, Tanzania. Children were randomly allocated three days of amodiaquine, amodiaquine +sulfadoxine−pyrimethamine, or amodiaquine+artesunate, or a 3−day six−dose regimen of artemether−lumefantrine. The primary endpoint was parasitological failure by day 14 assessed blind to treatment allocation. Secondary endpoints included day 28 follow−up and gametocyte carriage. Analysis was by intention to treat. Findings Of 3158 children screened, 1811 were randomly assigned treatment and 1717 reached the 14−day follow−up. The amodiaquine group was stopped early by the data and safety monitoring board. By day 14, the parasitological failure rates were 42 percent for amodiaquine, 20 percent for amodiaquine+sulfadoxine−pyrimethamine, 11 percent for amodiaquine+artesunate, and one percent for artemether−lumefantrine. By day 28, the parasitological failure rates were 76 percent, 61 percent, 40 percent, and 21 percent, respectively. The study shows how few the options there are for treating malaria where there is already a high level of resistance to sulfadoxine−pyrimethamine and amodiaquine.
Source: http://www.thelancet.com/journal/vol365/iss9469/full/llan.365.9469.primary_research.33055.1

17. *April 22, United Press International* — **New software speeds bioattack cleanup.** A new software tool, developed by scientists at New Mexico's Sandia National Laboratory, will help speed cleanup after a bioterror attack. The software is intended to guide the collection of samples used to plan post−attack cleanup and then determine if it has been effective. Speeding cleanup is one way to minimize the economic impact of terrorism. The software, called Building Restoration Operations Optimization Model or BROOM, is incorporated into a handheld device along with a contamination map and layout of the location where the responders are collecting samples. Also in the device are a barcode scanner and a wireless laser range finder to accurately identify where the sample was taken. The device stores data on where a sample was taken then transmits the information wirelessly to a computer outside the building. Because of safety concerns and heavy gear Hazmat workers can only stay in a building for a short time. BROOM helps make the most of their time.
Source: http://washingtontimes.com/upi−breaking/20050422−085431−4823 r.htm

[Return to top]

Government Sector

18. *April 22, GovExec* — **Park Service could get homeland security dollars.** Rep. Mark Souder (R−IN), chairman of the House Government Reform Subcommittee on Criminal Justice, Drug Policy and Human Resources, said Friday, April 22, that there is some agreement among congressional appropriators that the Park Service should receive additional funding for guarding 388 parks and 88 million acres of land throughout the United States. He did not specify whether that money would come out of the Department of Homeland Security's budget or from another source. "There is a significant amount of terrorist talk about the national icons," Souder told Government Executive. "The park rangers that are being pulled in to do homeland security are being pulled from somewhere else." For fiscal 2006, the Park Service budget request includes $2.2 billion in the Department of Interior appropriations for general operations and $320 million in the Department of Transportation appropriations for maintaining its 8,000 miles of roads. The Park Service must maintain its vast tracts of land along with rising personnel costs, aging facilities and growing homeland security concerns. Souder said the agency should not be forced to choose between providing services to park visitors and protecting those sites from potential terrorist attacks.
Source: http://www.govexec.com/dailyfed/0405/042205p1.htm

[Return to top]

Emergency Services Sector

19. *April 24, The Capital (MD)* — **Mock crash at BWI Airport trains rescuers.** Emergency workers from multiple counties took part in an emergency training exercise at BWI Airport in Maryland on Saturday, April 23. The exercise was the first time rescuers used the National Incident Management System, a set of response standards developed by the Department of Homeland Security, said R. Earl Lewis Jr., the assistant secretary for administration at the state's Department of Transportation. Gov. Robert L. Ehrlich Jr. mandated the use of the emergency management system statewide in an executive order issued last month. "That

prevents confusion of having a multi−agency response where the different organizations are using different incident management procedures," Lewis said. Since BWI's fire department is relatively small, any large−scale disaster will bring in authorities from nearby jurisdictions, Woodrow Cullum, chief of the BWI Airport Fire and Rescue Department, said. Getting everyone on the same page to ensure a smooth response is essential. This was the first time area hospitals were involved in the exercise. While there were no major problems, workers at North Arundel Hospital noticed five or six minor shortcomings, Carol Ann Sperry, the hospital's director of emergency nursing, said. Things like having water for victims' families and more stretcher ramps to get patients over curbs were needed, she said.
Source: http://www.hometownannapolis.com/cgi−bin/read/2005/04_24−57/ TOP

[Return to top]

Information Technology and Telecommunications Sector

20. *April 25, BBC News (UK)* — **Survey: Web server attacks 'growing fast'.** A survey by Zone−H revealed that web server attacks and Website defacements grew by 36% during 2004 when almost 400,000 incidents were recorded. The attacks include 49 separate sorties against U.S. military servers and huge numbers of Website defacements. The figures were collated by Zone−H , a web−based organization that uses a world−wide network of volunteers to spot and investigate web server attacks and site defacements. "Defacement is just one option for an attacker," said Roberto Preatoni, Zone−H coordinator. "In most circumstances the techniques used by defacers are the same techniques used by serious criminals to cause more serious damage." The report found that more than half of all attacks and defacements, 55%, succeeded by exploiting a known bug or vulnerability or an administration mistake. The figures show that the many incidents occur on the anniversaries (mid−March) of the start of the most recent war in Iraq when both pro−Muslim and pro−American groups defaced sites. The survey also found that the long holidays around Christmas provoke a spike in attacks and incidents. The frequency of attacks also dips around the time that schools re−open suggesting that many teenagers are behind the defacements.
Survey: http://www.zone−h.com/news/read/id=4457/
Source: http://news.bbc.co.uk/1/hi/technology/4480689.stm

21. *April 25, ZDNet (UK)* — **Trend Micro customers suffer weekend problems.** Trend Micro apologized on Monday, April 25, for distributing a faulty software update that caused IT workers around the world to spend the weekend fixing their systems. The Japan−based antivirus company has promised to compensate customers whose computers running Windows XP SP2 were disabled by the update. The company said the update was only available for ninety minutes and caused "certain performance issues" with CPUs. Trend Micro, which denied rumors that the update included a virus, said it didn't know what had caused the incident but that it had now issued a fix and was working with channel partners to solve the problem. Trend Micro said that most of the businesses affected were located in Japan, and that few complaints had been received from customers in the U.S. and Europe. The update affected versions 7.5 and above of Trend Micro's Scan Engine.
Source: http://news.zdnet.co.uk/0,39020330,39196220,00.htm

22.

April 25, ZDNet (UK) — **Hackers attack IT conference in London.** Hackers infiltrated an IT exhibition last week and attacked delegates' computers with a new type of wireless attack. Security experts attending the Wireless LAN Event in London last Wednesday, April 20, found that anonymous hackers in the crowd had created a Website that looked like a genuine login page for a Wi−Fi network, but which actually sent 45 random viruses to computers that accessed it. Spencer Parker, a director of technical solutions at AirDefense, said that the hackers walked around the exhibition carrying a Linux−based laptop running software that turned it into a wireless access point. The technique has evolved from an "evil twin" attack, where hackers host fake log−in Websites at commercial Wi−Fi hotspots. This was originally used to lure people into typing in credit card details onto the Web page, so the hacker could steal them.
Source: http://news.zdnet.co.uk/internet/security/0,39020375,3919595 6,00.htm

23. *April 22, Secunia* — **WebAPP E−Cart module shell command injection vulnerability.** A vulnerability has been reported in the E−Cart module for WebAPP, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "art" parameter in "index.cgi" isn't properly sanitised before being used in an "open()" call. This can be exploited to inject arbitrary shell commands via the "|" character. The vulnerability has been reported in version 1.1. Other versions may also be affected. There is no solution at this time.
Source: http://secunia.com/advisories/15054/

24. *April 22, SecurityFocus* — **Opera SSL security feature design error vulnerability.** Opera is prone to a design error that can result in a false sense of security. The source of the vulnerability is that the Organization Name of an SSL certificate is not intended to be unique. Since this field is not unique, it is not sufficient to use as a basis for the user to trust the authenticity of a Website. There is no solution at this time.
Source: http://www.securityfocus.com/bid/13176/discussion/

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: Multiple vulnerabilities have been reported in Firefox, which can be exploited by malicious people to conduct cross−site scripting attacks, bypass certain security restrictions, and compromise a user's system. Successful exploitation may allow execution of arbitrary code.

Current Port Attacks

Top 10 Target Ports	22321 (wnn6_Tw), 445 (microsoft−ds), 135 (epmap), 7674 (−−−), 1026 (−−−), 1025 (−−−), 80 (www), 41170 (−−−), 20525 (−−−), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[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:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security 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. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

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 a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.