



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 25 March 2005

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports that seven children in Florida have contracted a life-threatening kidney infection that health officials said may be the result of a rare infection picked up at petting zoos. (See item [16](#))
- Fast-track recruitment has begun for a trial to investigate the safety of a vaccine against H5N1 avian influenza, the National Institute of Allergy and Infectious Diseases announced Wednesday. (See item [18](#))

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: [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. *March 24, Associated Press* — **Ground broken on new gas terminal in Louisiana.** Federal energy regulators and state officials have broken ground in Cameron Parish, LA, on the country's newest and largest liquefied natural gas (LNG) terminal. The terminal will be built on a 568-acre site about four miles up the Sabine River on the state line. The remote locale has nearly as many pipelines as people. Huge tankers will transport the gas in super-cooled liquid form to make for easy transport to the terminal where it will be converted back to gas and sent by pipeline to the rest of the country. Officials from Cheniere Energy, the owner of the facility, say that two of the LNG ships will be able to dock simultaneously at the terminal, which could be operating by 2008. The terminal will have the capacity to handle 2.6 billion cubic feet per

day -- more than any of the four domestic LNG terminals now operating.

Source: <http://www.katc.com/Global/story.asp?S=3120326>

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

Chemical Industry and Hazardous Materials Sector

Nothing to report.

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

Defense Industrial Base Sector

Nothing to report.

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

Banking and Finance Sector

2. *March 24, Associated Press* — Washington state computer worm affects tax transactions.

A computer worm that infected the Washington state Revenue Department's system caused some businesses to be charged twice for their taxes. The department has reversed 1,400 faulty transactions, Deputy Director Ralph Osgood said. "No confidential taxpayer information was compromised, no data was lost and there was no loss of funds," he said. The worm entered the Revenue Department's computer system on Monday, March 21, and soon infected all 13 of its offices statewide. The worm shut down the network, which affected the department's billing system. Instead of flagging the accounts of businesses that paid their taxes over the Internet, the system mistakenly didn't flag those accounts and charged the businesses for their taxes a second time. The state's computer experts sealed off the Department of Revenue from the rest of the state's computer systems when the worm was detected on Monday, so the problems haven't spread to other government agencies. Osgood said officials don't know where the computer worm originated.

Source: http://www.kgw.com/business/stories/kgw_032305_biz_revenue_virus.16921e2ee.html

3. *March 24, ZDNet (Australia)* — Phishers target Yahoo instant messenger users. Yahoo's free instant messaging service is being targeted by phishers in an attempt to steal usernames, passwords and other personal information. Yahoo confirmed on Thursday, March 24, its service was being targeted by a phishing scam. According to the search company, attackers are sending members a message containing a link to a fake Website that looks like an official Yahoo site and asks the user to log in by entering their Yahoo ID and password. The scam is convincing because the original message seems to arrive from someone on the victim's friends list. Should the recipient of the phishing message enter their details, the attackers can gain access to any personal information stored in their profile and more importantly, the victim's contact lists. A Yahoo spokesperson said the attack was not very widespread but consumers should be aware it exists so they can protect themselves.

Source: <http://news.zdnet.co.uk/internet/security/0.39020375.3919257.8.00.htm>

4. *March 23, Federal Reserve Board* — **Federal bank and thrift regulatory agencies jointly issue interagency guidance on response programs for security breaches.** The federal bank and thrift regulatory agencies have jointly issued Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. The guidance interprets the agencies' customer information security standards and states that financial institutions should implement a response program to address security breaches involving customer information. The response program should include procedures to notify customers about incidents of unauthorized access to customer information that could result in substantial harm or inconvenience to the customer. Under the guidance, a financial institution should notify its primary federal regulator of a security breach involving sensitive customer information, whether or not the institution notifies its customers. The guidance is being issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. Federal Register Notice: <http://www.federalreserve.gov/BoardDocs/Press/bcreg/2005/20050323/attachment.pdf>
Source: <http://www.federalreserve.gov/BoardDocs/Press/bcreg/2005/20050323/default.htm>

5. *March 23, ZDNet (UK)* — **UK bank customers becoming more phishing savvy.** The UK Association of Payment and Clearing Services (APACS) has claimed that banking customers are waking up to the threats of online fraud. An APACS spokesperson said on Wednesday, March 23, that although last year's figures for online fraud were high, only a few people were hit. This is due to growing awareness about phishing scam e-mails, which are sent by criminals pretending to be officials from banks or online shops, APACS believes. "Increasingly customers are realizing that banks don't communicate this way and that they shouldn't respond to fraudsters," said Sandra Quinn, director of corporate communications for APACS. "We're not surprised that last year's losses are high because of the number of attacks that have been made. What is encouraging is that it affected only a very small number of victims." APACS reported earlier this month that banks lost US\$22 million through online fraud last year, as consumers fell victim to identity theft e-mail scams. An APACS report on card fraud stated that phishing scams in particular were responsible for online financial crime, although identity theft and check fraud also contributed to the figure.
Source: <http://news.zdnet.co.uk/internet/security/0.39020375.3919256.0.00.htm>

6. *March 22, This is London (UK)* — **Alert over bank virus.** Online bank customers are at risk from a computer virus which directs them to fake financial Websites, experts warned Monday, March 21. The threat is from a virus called Troj/BankAsh-A, which has been halted by filters 40,000 times since it appeared on the Internet last month. If downloaded, the virus lies dormant until the user tries to access a banking Website. The user is then directed to a fake site which looks like the real thing. Criminals use data entered to raid the user's bank account.
Source: <http://www.thisislondon.com/news/articles/17411374?source=EveningStandard>

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

Transportation Sector

7. *March 24, Department of Transportation* — **Agency proposes plan to improve Midwest rail network.** A project to improve and expand passenger rail service throughout the Midwest could

have a partner in the federal government for the first time under the Bush Administration's proposal to reform Amtrak, Transportation Secretary Norman Y. Mineta said during a news conference at the Detroit railroad station on Thursday, March 24. Mineta unveiled details of the Administration's Amtrak reform proposal, the Passenger Rail Investment Reform Act. Mineta said the Administration's plan to establish 50–50 federal matching grants for state investments in passenger rail infrastructure, like stations, trains and track. These grants would help fund projects like the Midwest Regional Rail Initiative and give states an incentive to invest in better tracks and more reliable equipment, making trains more popular and profitable, decreasing the need for states to pay operating subsidies, Mineta added. The proposal, Mineta said, would will free Amtrak of the cost of maintaining tracks and stations, allowing the company to focus on running the trains. The plan would also introduce competition for rail service by letting states chose operators to run key routes.

Source: <http://www.dot.gov/affairs/dot5205.htm>

8. *March 24, Miami Herald (FL)* — **Computer outage delays flights at two Florida airports.** A 30–minute computer system outage at Miami International Airport (MIA) on Wednesday, March 23, delayed flights in and out of at least two South Florida airports for up to two hours. The malfunction interrupted an automatic transfer of information between the control tower radar room at MIA and the region's air traffic control center, said Kathleen Bergen, public affairs manager for the Federal Aviation Administration in Atlanta, GA, forcing controllers to handoff air traffic manually by making phone calls. After the problem was corrected, technicians had to wait 30 minutes to allow controllers to guide airplanes already in the air to safe landings before rebooting the computer system, Bergen said. In Broward, where the system outage was made worse by stormy weather, 23 inbound and outbound flights scheduled for Fort Lauderdale–Hollywood International Airport experienced delays, said airport spokesperson Jim Reynolds.

Source: <http://www.miami.com/mld/miamiherald/news/11214768.htm>

9. *March 23, Government Executive* — **Panel discusses inland port security.** Focus on shipping containers as potential Trojan horses for a WMD attack on the United States could be diverting needed attention from other seaborne threats, lawmakers and witnesses said at a field hearing on the subject Tuesday, March 22, in Vicksburg, MS. In an interview following her testimony at the hearing, Inland Rivers, Ports and Terminals Association Executive Director Deirdre McGowan said that inland ports do not get the attention that ocean ports receive even though the former can be more vulnerable, since they tend to be longer. About 4 percent of federal port security grant money goes for inland ports, McGowan said. She called for a renewed commitment to inland ports, including for use as test grounds for new technologies and new approaches to port security. McGowan stressed the importance of basing port security funding on risk, and she acknowledged that high–profile threats such as radiological weapons are not as applicable to inland ports as ocean ports. She also called for a greater focus on conventional weapons that could have a serious economic effect on river commerce.

Source: <http://www.govexec.com/dailyfed/0305/032305gsn1.htm>

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

Postal and Shipping Sector

10. *March 24, L.A. Daily News (CA)* — **Los Angeles Police Department targets mailbox firms in identity thefts.** Overwhelmed with 10,000 complaints of identity theft a year, Los Angeles, CA, police launched a campaign Tuesday, March 23, against private mailbox companies that fail to comply with customer–screening laws. The Los Angeles Police Department is teaming with the City Attorney's Office to identify and prosecute companies that fail to keep two forms of identification on file for anyone who uses a private mailbox. The owners are also required to return or destroy mail that arrives for an addressee not listed in their files. Police previously issued only a warning when they suspected a mailbox of being a hub for identity thieves. Now they plan to force owners to comply, with the threat of jail time and a \$2,500 fine. Business owners who violate the law provide mail recipients with a level of anonymity that creates a perfect environment for identity theft, City Attorney Rocky Delgadillo said.
Source: <http://www.dailynews.com/Stories/0.1413,200~20954~2777243.00.html>

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

Agriculture Sector

11. *March 24, Associated Press* — **Wasting disease plan insufficient, federal official says.** A state plan for addressing chronic wasting disease (CWD) if it turns up on Wyoming's elk feedgrounds is a good first step but doesn't go far enough, says a disease expert with the U.S. Fish and Wildlife Service. The plan acknowledges that while infection rates among free–ranging elk is around three percent, it can exceed 50 percent in captive elk. The implication is that feedground elk, which are artificially concentrated like captive animals, could also have higher disease rates. Tom Roffe, the federal agency's chief of wildlife health, praises the Wyoming Game and Fish Department for acknowledging that the 23 state elk feedgrounds could help spread CWD. But he said the proposals would come too little, too late to protect elk. Researchers suspect the disease spreads through animal–to–animal contact. The plan recommends keeping feedgrounds open even after CWD is discovered, although feeding areas would be spread out and feeding days cut back to disperse elk. While Roffe praised those goals, he warned that Wyoming should not wait until the disease reaches feedgrounds.
Source: <http://www.casperstartribune.net/articles/2005/03/24/news/wyoming/c9430cfdc7b6dbf987256fcb004c4657.txt>
12. *March 23, Associated Press* — **Monsanto completes purchase of Seminis.** St. Louis, MO, based Monsanto Co. said Wednesday, March 23, it has completed its billion–dollar cash purchase of Seminis Inc., the world's largest developer, grower and marketer of fruit and vegetable seeds. As part of the deal announced in January, Monsanto will assume \$400 million in debt by Seminis, supplier of more than 3,500 seed varieties to commercial fruit and vegetable growers, dealers, distributors, and wholesalers in more than 150 countries. Seminis will be a wholly owned Monsanto subsidiary, and remain based in Oxnard, CA.
Source: http://seattlepi.nwsource.com/business/apbiz_story.asp?category=1310&slug=Monsanto%20Seminis
13. *March 23, Agriculture Online* — **Southeastern U.S. weather favors spread of soybean rust spores.** Weather conditions in the Southeast this week have created a "serious threat" for spread of soybean rust in the region, according to The North American Plant Disease Forecast Center at North Carolina State University. The center issued a report on Monday, March 21, saying

"sky conditions were highly favorable for spore survival." A weather system this week featuring heavy rains was expected to deposit airborne spores on Monday, March 21, and Tuesday, March 22. The conditions were producing a "strongly moderate risk" for susceptible plants in central and northern Florida, central and southern Georgia, and eastern Alabama. Other parts of the region were regarded as low risk.

Source: http://www.agriculture.com/ag/story.jhtml?storyid=/templatedata/ag/story/data/agNews_050323jwRUSTRISK.xml&catref=ag1001

14. *March 23, AgWeb* — **New rapid test for soybean rust created.** A Portland, ME, company recently announced that it had developed a rapid test for detecting soybean rust. The company has developed an immunodiagnostic test for soybean rust. It is based on a laboratory assay that takes around two hours to perform, and it will provide a qualitative (presence/absence) answer. This new test gives diagnostic laboratories the ability to quickly and reliably screen for the disease. The test kit can detect one symptomatic leaf spot caused by the disease at a very early stage, before the development of a pustule and sporulation. During this period it is often difficult to differentiate leaf spot symptom from other bacterial, viral, and fungal infections. In addition to the laboratory test, the company is also finalizing development of a five-minute test strip for in-field testing.

Source: http://www.agweb.com/get_article.asp?pageid=116413

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

Food Sector

Nothing to report.

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

Water Sector

15. *March 23, Associated Press* — **Pipeline rupture spills oil into California reservoir.** A landslide apparently ruptured a light crude oil pipeline located about 60 miles northwest of Los Angeles, CA, Wednesday, March 23, spilling up to 126,000 gallons into a reservoir that provides water to Southern California cities, officials said. Officials said they had cordoned off the affected area of Pyramid Lake and were not concerned about potential contamination of the region's drinking water. "These kinds of spills are usually pretty localized," said Henry Martinez, chief operating officer for the Los Angeles Department of Water and Power, which uses water from the reservoir to generate power. Firefighters closed several lanes of Interstate 5, a major north-south highway, as they rushed to isolate the area and build a dike to keep more oil from pouring into the lake. The Forest Service and state Department of Fish and Game were working with pipeline owner Pacific Energy Partners to control the oil.

Source: <http://www.signonsandiego.com/news/state/20050323-2317-oilspill.html>

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

Public Health Sector

16. *March 24, Associated Press* — Florida investigates illnesses after zoo visits. Seven children have contracted a life-threatening kidney infection that health officials said may be the result of a rare infection picked up at petting zoos. Five of the seven were hospitalized in critical condition, including one on dialysis. Another had been upgraded to stable condition, said Mehul Dixit, who is treating some of the children at Florida Hospital Orlando. One child was treated at Arnold Palmer Hospital for Children & Women and released several weeks ago. The children all touched animals recently at area fairs, including the Central Florida Fair in Orlando and the Florida Strawberry Festival in Plant City. They might have been exposed to the bacteria through the animals' feces, officials said. The potentially dangerous kidney condition — hemolytic uremic syndrome, or HUS — is a rare complication arising from an infection most commonly associated with *E. coli*, a bacterium found in undercooked beef or contaminated food. Bill Toth, a spokesperson for the Orange County Health Department, said not all the children showed signs of *E. coli* exposure, and investigators were running additional tests. Officials said three of the children tested positive for a different bacterium — *Staphylococcus aureus* — that can sometimes lead to the kidney problem.

Source: http://www.sun-sentinel.com/news/nationworld/ats-ap_health19_mar24.0.5063886.story?coll=sns-ap-tophealth

17. *March 24, Agence France Presse* — Bird flu claims second victim in Cambodia. A 28-year-old Cambodian has died of bird flu at a hospital in the capital to become the country's second victim of the virus, the health minister, Nuth Sokhom, said. The victim came from Kampot province which borders Vietnam. His village of Tram Sasor is 12 miles from the home of the first victim, a woman aged 25 who died in January while being treated in Vietnam. Yim Voerunthan, secretary of state at the ministry of agriculture, said more than 600 chickens had died in six villages in Kampot in the last 20 days and a further 120 had been culled Wednesday, March 23, with 55 houses being disinfected. Directors of the eight Pasteur Institutes from across the Asia-Pacific region were to meet in the Cambodian capital Monday, March 28. They will work to update and standardize their diagnosis methods for bird flu. More information about avian influenza is available from the U.S. Centers for Disease Control and Prevention: <http://www.cdc.gov/flu/avian/>

Source: <http://health.news.designerz.com/bird-flu-claims-second-victim-in-cambodia.html?d20050324>

18. *March 23, National Institute of Allergy and Infectious Diseases* — Trial of experimental avian flu vaccine. Fast-track recruitment has begun for a trial to investigate the safety of a vaccine against H5N1 avian influenza, the National Institute of Allergy and Infectious Diseases (NIAID), part of the National Institutes of Health (NIH), announced Wednesday, March 23. Sites in Rochester, NY, Baltimore, MD, and Los Angeles, CA, will enroll a total of 450 healthy adults. The clinical sites are part of the NIAID-sponsored Vaccine and Treatment Evaluation Units (VTEU). Sanofi pasteur, of Swiftwater, PA, manufactured the trial vaccine, which is an inactivated vaccine made from an H5N1 virus isolated in Southeast Asia in 2004. This Phase I trial will test the vaccine's safety and ability to generate an immune response in 450 healthy adults aged 18 to 64. If the vaccine is shown to be safe in adults, there are plans to test it in other populations, such as the elderly and children. H5N1 avian influenza leads to severe disease in both birds and humans. Between January 2004 and March 11, 2005, there were 69 confirmed cases of and 46 deaths from H5N1 infection in humans reported to the World Health Organization.

Source: <http://www2.niaid.nih.gov/newsroom/Releases/avianfluvax.htm>

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

Government Sector

19. *March 23, Federal Computer Week* — **Selling e–gov to agencies.** Agency officials will bolt away from common e–government solutions at the first available opportunity unless the online solution is cheapest service possible, a grants.gov official said Wednesday, March 23. Organizations will naturally gravitate toward applications created specifically for them, said Rebecca Spitzgo, grants.gov program manager for the Health and Human Services Department. Because of the resistance to shared solutions, e–government has to save money, she said. When officials must pay for e–government through interagency fee for service, "we have to keep the costs ... not only reasonable, but cheaper than they could do it for themselves," Spitzgo said at a seminar in Washington, DC. As a result, e–government solutions need be economically–designed, Spitzgo said. The complexities of expensive bells and whistles present another factor that hinders wide adoption, Spitzgo said. E–government has to be easy enough to use that designers can release the product with confidence that users will figure out how to operate it without agency training.

Source: <http://www.fcw.com/article88382-03-23-05-Web>

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

Emergency Services Sector

20. *March 25, First Response Coalition* — **Report finds first responders underfunded.** Police, fire and EMT needs will be underfunded by about \$100 billion through 2008, according to a new report from the First Response Coalition titled "America's First Responders and the Federal Budget: A Study of Rhetoric Versus Reality." The reports states that this estimate is based on budget figures for the Department of Homeland Security and does not take into account any cuts to first responder funds that reside in other federal departments. According to the report: fire departments across the country have only enough radios to equip half the firefighters on a shift, and breathing apparatuses for only one third; police departments in cities across the U.S. do not have the protective gear to safely secure a site following an attack with weapons of mass destruction; and most cities do not have the necessary equipment to determine what kind of hazardous materials emergency responders may be facing.

Source: <http://www.firstresponsecoalition.org/release-03-23-2005.sht ml>

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

Information Technology and Telecommunications Sector

21. *March 24, Computerworld* — **FBI asks companies to report cyber intrusions.** Corporate executives are often reluctant to report network intrusions for fear of having those security breaches made public and drag down stock prices. But state and federal law enforcement officials who spoke at an information security panel in New York on Wednesday, March 23,

said such reports can sometimes provide an important missing link in larger cybersecurity investigations. "It may be a critical piece of information you're submitting to us – you never know where that fits into the pie," said Ron Layton, section chief of the cyber coordination branch for the Department of Homeland Security (DHS). Layton was one of several law enforcement officials who spoke at an information security conference sponsored by AIT Global Inc. and InfoWorld Media Group. Network intrusion reports don't necessarily have to fall within the statutory \$5,000 minimum loss for federal authorities to investigate them, said Kent McCarthy, a special agent for the Secret Service in New York. McCarthy said the Secret Service does its best to protect the anonymity of corporations that report network intrusions. "We're not looking for a press release," he said. DHS cyber coordination branch: <http://www.uscert.gov> and Secret Service: <http://www.ustreas.gov/uss/index.shtml>
 Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,100598,00.html>

22. **March 23, K–Otik Security — Mozilla Suite/Firefox/Thunderbird code execution vulnerabilities.** Several vulnerabilities were identified in Mozilla Suite, Firefox and Thunderbird, which may be exploited by attackers to execute arbitrary commands or bypass certain security features. These vulnerabilities are due to a heap overrun error, an error in bookmarking a specially crafted page as a Firefox sidebar panel, and an error when handling specially crafted XUL files. Update to the most current version of the product: <http://www.mozilla.org>
 Source: <http://www.k-otik.com/english/advisories/2005/0296>

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: US–CERT has identified a recent increase of reported P2P incidents. P2P file sharing technology provides Internet users with the potential to share local files with a potentially unlimited number of other Internet users. As a result, the usage of P2P software may allow for sensitive data or personal information to be leaked from computer systems. Further, P2P may provide a vector for malicious code to be introduced into an enterprise environment.	
Current Port Attacks	
Top 10 Target Ports	445 (microsoft–ds), 135 (epmap), 1026 (----), 6346 (gnutella–svc), 53 (domain), 1027 (icq), 80 (www), 1025 (----), 139 (netbios–ssn), 2234 (directplay) 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

23. *March 23, U.S. Department of State* — U.S. Department of State issues travel warning for the Philippines. The State Department has issued a Travel Warning recommending that Americans consider carefully the risks of travel to the Philippines. Terrorist groups, including Jemaah Islamiyah and the Abu Sayyaf Group, and radical elements of the Moro Islamic Liberation Front are planning multiple attacks throughout the Philippines. This information has been also released by Philippine government officials and is in the Philippine media. The Department urges Americans who choose to travel to the Philippines to observe vigilant personal security precautions; to remain aware of the continued potential for terrorist attacks against Americans, U.S. or other Western interests in the Philippines, and to register with the U.S. Embassy. The Department warns against all but essential travel throughout the country in light of a heightened threat to Westerners. There has recently been an increase in bombings by the terrorist groups in Manila, the region of Mindanao, and other areas where terrorist groups are active. Bombs have exploded in shopping malls, on public transportation, at airports and port facilities, in places of worship, and in other public areas resulting in numerous casualties, including several deaths. Bombs have also been found at places of worship.

Source: http://travel.state.gov/travel/cis_pa_tw/tw/tw_2190.html

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

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

[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. 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.