Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 10 May 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 Daily News reports this season's near−record rainfall in California has spawned fears of a widespread outbreak of potentially deadly West Nile virus and more than a dozen other mosquito−borne viruses. (See item 18)
- NewScientist reports a brief blackout at Internet search giant Google has drawn attention to the addressing system that underpins the Web: the Domain Name System which maps Web names to the numerical Internet Protocol addresses used by computers. (See item 22)

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. *May 09, Associated Press* — **Duke Energy to buy Cinergy.** Duke Energy Corp. said Monday, May 9, it has agreed to acquire Cinergy Corp. for stock valued at about $9 billion in a deal that will create an energy company with about 5.4 million retail customers and more than $70 billion in assets. The deal was unanimously approved by both companies' boards. The combined company will have about $27 billion in annual revenue and $1.9 billion in annual net income. It will own or operate about 54,000 megawatts of electric generation domestically and internationally. Duke Energy, based in Charlotte, NC, is a diversified energy company with natural gas and electric businesses as well as a real estate portfolio. Cinergy, based in Cincinnati, OH, operates Cincinnati Gas & Electric Co., Union Light, Heat & Power and PSI

Energy. Following the completion of the deal, the company will be based in Charlotte, NC. Local headquarters of the operating utilities will remain unchanged by the merger.
Source: http://www.nytimes.com/aponline/business/AP−Cinergy−Duke−Ene rgy.html?

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *May 09, Associated Press* — **Chemical plant explodes in Oregon.** Three people at Lacamas Labs chemical plant that exploded in north Portland Monday morning, May 9, are being decontaminated by hazardous materials teams. The explosion happened at about 4:15 a.m. About 200 employees of a Nordstrom warehouse were evacuated after the industrial fire at the chemical plant that makes pharmaceuticals. The U.S. Coast Guard was on the scene, concerned the chemicals could go into the Columbia River because of a water main break.
Source: http://www.koin.com/news.asp?ID=2475

3. *May 09, Associated Press* — **Grounded barge leaks diesel into Virginia river.** A barge that ran aground in the James River, near Richmond, VA, spilling an undetermined amount of fuel, was transferring more than 44,000 barrels of diesel fuel Monday, May 9, as the Coast Guard sought the cause of the grounding. While the environmental impact of the spill had not been fully assessed, there were no reports of fish kills or birds fouled by the fuel, said Jerry Crooks, a spokesperson for the Coast Guard in Norfolk, VA. The 300−foot barge, owned by Vane Line Bunkering of Baltimore, had just picked up its cargo south of Richmond Sunday morning when it ran aground. An initial estimate put the spill at approximately 200 gallons. "All of the fuel has been contained in primary and secondary booms," Crooks said.
Source: http://home.hamptonroads.com/stories/story.cfm?story=86171&r an=167047

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *May 09, The Dominion Post (New Zealand)* — **Spear phishers evade usual spam defenses.** Internet scammers are turning to a new method of fooling the public −− spear phishing −− that evades traditional anti−phishing defenses. Generic phishing spams thousands of addresses with similar e−mails, usually asking the recipients to update their bank or PayPal Internet payment accounts through a realistic, but fake, Website. Spear phishing is more specific, typically targeting just a handful of people who are employees of an organization. In one method, the phisher harvests specific e−mail addresses, either through a phone call or through a company Website, and then sends four or five employees a message from a spoofed address purporting to be part of their IT or human resources department. This message directs the employees to enter their network password into a fake Website. With this information the hacker can access the

network and steal company funds or even intellectual property, depending on their motives. Traditional defenses against phishing don't block spear−phishing attempts because they are not mass mailed.
Source: http://www.stuff.co.nz/stuff/0,2106,3274129a28,00.html

5. *May 09, ComputerWeekly* — **Banking Trojan spreading rapidly.** Web portal Lycos is warning users of a rapidly spreading Trojan virus that tries to direct users to fake banking sites. Lycos said Barclays and Bank of Scotland are the latest banks to see their sites copied and users directed to the fakes, where their log−ins and passwords can be recorded for fraud. Last month, Lycos said it tracked and stopped 3.3 million attempts to load the Troj/BankAsh−A malware. "The stolen details are used to hi−jack bank accounts and for identity theft," said Wessel van Rensburg, Lycos UK head of e−mail. Troj/BankAsh−A is distributed via an e−mail attachment. Once opened the user's machine downloads the malware from a malicious Website. It then remains undetected on the machine until the user tries to log−in to a banking Website. However, even if users type in the correct domain name for the banking site they want, they are not linked to that site as hackers have managed to change the configurations of internet domain name servers. Users with the Trojan are instead directed to a different Internet Protocol address to the one normally associated with the legitimate Website.
Source: http://www.computerweekly.com/articles/article.asp?liArticleID=138382&liFlavourID=1&sp=1

[Return to top]

Transportation and Border Security Sector

6. *May 09, Associated Press* — **Study: Traffic jams increasing.** The Texas Transportation Institute is reporting that gridlock is getting worse. Congestion delayed travelers 79 million more hours and wasted 69 million more gallons of fuel in 2003 than in 2002, the Institute's 2005 Urban Mobility Report said. Overall in 2003, there were 3.7 billion hours of travel delay and 2.3 billion gallons of wasted fuel for a total cost of more than $63 billion. "Urban areas are not adding enough capacity, improving operations or managing demand well enough to keep congestion from growing," the report concluded. Congestion can also be reduced by managing traffic better. The report said such techniques as coordinating traffic signals, smoothing traffic flow on major roads and creating teams to respond quickly to accidents reduced delay by 336 million hours in 2003. Tim Lomax, a co−author of the report, said the soft economy and slow job growth in 2003 meant that congestion got worse more slowly than it would have during better times. Only job loss or major commitments to expand capacity will decrease congestion dramatically, he said. Refusing to build more roads and transit systems won't discourage population growth, Lomax said.
Urban Mobility Study: http://mobility.tamu.edu/ums/
Source: http://www.abqtrib.com/albq/nw_local/article/0,2564,ALBQ_19858_3763541,00.html

7. *May 09, Associated Press* — **Alaska truckers enlisted in watch for terrorists.** About 700 Alaska truckers have been trained to watch the highways they drive for terrorist activities. The drivers are part of Highway Watch, a nationally organized, federally funded program that is run by the state and led by the industry's trade group, the American Trucking Association. There are many potential terrorist targets in Alaska, terrorist expert and trainer of Highway Watch

Ray Brown said in an interview after the session. "Alaska's energy resources are considerably important, not only to Alaska but to the Lower 48," he said. There's also the pipeline. Alaska is an international state, with a lot of international travelers coming through the airport, and the huge amount of cargo moving through the ports also offers opportunities, he added. The Alaska drivers, along with 75,000 truckers from around the nation, are part of Highway Watch, a nationally organized, federally funded program that is run by the state and led by the industry's trade group, the American Trucking Association. The Transportation Security Administration began funding the program in October 2004.
Source: http://www.juneauempire.com/stories/050905/sta_20050509007.s html

8. *May 09, Union Leader (NH)* — **New Hampshire airport evacuated after bomb threat.** A bomb threat prompted evacuation of the passenger terminal of Manchester Airport for about 90 minutes on Sunday afternoon, May 8, inconveniencing hundreds of travelers and delaying flights. Airport officials would not discuss in detail the threat that prompted the evacuation. "Within 25 minutes of bringing people back into the building, everyone was reprocessed through security," said airport Director Kevin Dillon. Security teams swept through the airport after it was cleared and found no bomb, officials said. And things did get back to normal quickly −− just after 3 p.m., only a handful of arriving and departing flights were still delayed.
Source: http://www.theunionleader.com/articles_showfast.html?article =54472

9. *May 06, Government Accountability Office* — **GAO−05−423SP: Highlights of an Expert Panel: The Benefits and Costs of Highway and Transit Investments (Special Publication).** The nation’s economy and its citizens’ quality of life depend on our transportation system. While all government levels have made significant investments in transportation, projections of future passenger and freight travel indicate that considerable investment will be needed to maintain the system. However, this comes amid growing concern about the size of the federal budget deficit and increasing demands on state and local government revenue. As a result, careful decisions will need to be made to ensure that transportation investments maximize the benefits of each dollar invested. The House Appropriations Committee report accompanying the fiscal year 2004 Departments of Transportation and Treasury and Independent Agencies Appropriations Bill, required the Government Accountability Office (GAO) to review the benefits and costs of various transportation modes. As part of this study, GAO convened an expert panel that included some of the leading transportation economists and practitioners from throughout the nation. The panel discussed the benefits and costs of highway and transit investments. GAO asked expert panel participants to discuss how to conceptualize, measure, improve, and use information about the benefits and costs of highway and transit investments. The expert panel was not designed to reach a consensus on these issues, but several themes emerged from the panel’s discussion.
Highlights: http://www.gao.gov/highlights/d05423sphigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−423SP

10. *May 03, Republic Mexico City Bureau* — **Canada wants Mexican immigrants.** As the United States fortifies its border with Mexico, Canadian companies are reaching out to immigrants who are frustrated by U.S. restrictions and tempted by dreams of a better life in Canada. The Canadian government has been relaxing its immigration rules in an effort to attract students and skilled workers from all over the world. That, and the push by companies promising jobs and visas, is attracting Mexican professionals turned off by the Minuteman Project, new border

walls, tougher U.S. entry requirements and laws like Proposition 200 in Arizona. "Live in Canada!" says a Mexico City newspaper ad placed by a Canadian labor recruiter, as a photo of the Toronto skyline beckons. The reason, immigration experts say, is that Canada needs more people. "Our population is shrinking and getting older," said David Rosenblatt, a Canadian immigration lawyer whose firm advertises in Mexico. "Canada, in order to survive and grow, needs to get more skilled workers." Mexicans can enter Canada just by showing a passport, much easier than the long, expensive process of getting U.S. visas. Canada also has a widely praised farm worker program and is aggressively courting foreign students.
Source: http://www.azcentral.com/specials/special03/articles/0503can ada03.html

[Return to top]

Postal and Shipping Sector

11. *May 09, The Beacon News (IL)* — **Post offices plan bioterrorism drill.** A simulated disease will be sent through the mail in late May to train two regional post offices in DuPage County, IL, for the threat of bioterrorism, county health officials said. Leland Lewis, DuPage County Health Department executive director, said the drill is meant to test systems put into place since the October 2001 anthrax attacks at East Coast postal centers. The exercise will test biohazard alarm systems and emergency response at a surprise time and at an undisclosed location, he said. Staff members from the Health Department then will set up a medication dispensing site for the mock victims. The cost of the drill, along with other emergency preparedness plans, will be covered as part of $1.1 million in grants from the federal Centers for Disease Control and Prevention.
Source: http://www.suburbanchicagonews.com/beaconnews/top/a09postoff .htm

[Return to top]

Agriculture Sector

12. *May 09, U.S. Department of Agriculture* — **Two biotechnology reports issued.** The U.S. Department of Agriculture (USDA) on Monday, May 9, issued two reports on agricultural biotechnology that cover the evolving world requirements for the traceability and labeling of agricultural biotechnology products and on the complexities of predicting the use of these products in the future. The reports were developed by USDA's Advisory Committee on Biotechnology and 21st Century Agriculture (AC21).
Global Traceability and Labeling Requirements for Agricultural Biotechnology−Derived Products: Impacts and Implications for the United States:
http://w3.usda.gov/agencies/biotech/ac21/reports/tlpaperv37f inal.pdf
Preparing for the Future: http://w3.usda.gov/agencies/biotech/ac21/reports/scenarios−4 −5−05final.pdf
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?conten tidonly=true&contentid=event_15.xml

[Return to top]

Food Sector

13. *May 09, just−food.com* — **Brazil suspends beef exports to U.S.** Officials in Brazil's Agriculture Ministry temporarily suspended the country's processed beef exports to the U.S. as of May 5, according to a report from its Department of Livestock Farming Products Inspection quoted by Latin America News Digest. The measure has been taken in an attempt to meet U.S. requirements on the sanitary inspection of Brazilian establishments authorized to export beef meat to that country. A U.S. technical delegation in Brazil between March and April 2005 found irregularities in the sanitary inspection of local beef processing plants exporting to the USA. As a result, U.S. officials withdrew the license of three Brazilian beef exporters and temporarily suspended imports from five others in early April 2005. Brazilian authorities expect the beef exports to the U.S. to be restored within three weeks.
Source: http://www.just−food.com/news_detail.asp?art=60674

14. *May 07, Associated Press* — **Food commission's decision in Japan could lead to lifting of ban on U.S. beef imports.** Tokyo's food safety commission on Friday, May 6, said it would recommend the government waive mad cow disease tests for cattle younger than 21 months, a move toward lifting the ban on American beef imports to Japan. The decision follows mounting pressure from the United States on Japan to lift the embargo, which has deprived U.S. beef producers of their most lucrative overseas market. Tokyo has tested all cattle for the disease since discovering its first case of the fatal bovine illness in 2001. After the United States' discovery of its first mad cow case in December 2003, Japan stopped importing U.S. beef and demanded that Washington also adopt blanket testing for its herds. Japan's agriculture and health ministries will now review the commission's recommendations. Separately, they will hold public hearings in mid−May to explore the possibility of permitting U.S. beef into the country, said Yasuhiko Nakamura, a commission member. The food safety panel will then consider whether it's safe to reopen Japan's markets to U.S. beef before another round of public hearings, agriculture ministry official Hiroaki Ogura said.
Source: http://www.detnews.com/2005/business/0505/07/biz−174222.htm

15. *May 06, U.S. Food and Drug Administration* — **Sandwiches recalled in Missouri.** Quik'n Tasty Foods Inc. of Belton, MO, is recalling Po Boy (Lunchmeat, Ham and Cheese sandwiches) ink stamp dated 101 N6, because it has the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Po Boy sandwiches were distributed through Quicktrip convenience stores located in Missouri, Kansas, Illinois and Arizona, between April 18, 2005 and April 29, 2005. No illnesses have been reported to date.
Source: http://www.fda.gov/oc/po/firmrecalls/quikntasty05_05.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

16. *May 09, Agence France−Presse* — **Bird flu vaccine to be tested on humans in Vietnam.** A bird flu vaccine developed in Vietnam will be tested on humans next month amid fears that the disease could become a pandemic if it became easily transmittable between humans, a Vietnamese scientist said. "The first tests on human will be conducted in either late June or early July," Nguyen Thu Van, a key member of the group developing the vaccine said, adding that the results of tests on monkeys in February were "very good." "We expect to produce the human bird flu vaccine in early 2006," she said. Several other countries are carrying out research on bird flu vaccine. The World Health Organization said earlier this year it would make sure all laboratories shared their results to speed up chances of finding a vaccine. World health experts have warned that the H5N1 virus could lead to a global pandemic if it mutated into a form that was easily transmitted between humans.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050509/wl_asia_afp/healthfluvietnam_050509081954

17. *May 08, Canadian Press* — **Bird flu tests out−of−date, may have missed positive cases, scientists admit.** A diagnostic test designed by Canadian researchers and used in Vietnam to detect H5N1 avian flu is out of date, scientists from the National Microbiology Laboratory admit −− raising the possibility some human cases may have been dismissed in error. The test was designed at the Winnipeg lab using genetic sequencing information from samples of the virus that circulated in the first quarter of 2004. However, the virus has changed enough since then that questions have surfaced about the test's sensitivity. Tracking the virus's forays into and among humans is critical, given fears that H5N1 may acquire the ability to easily transmit from person to person, sparking an influenza pandemic. A scientist from the Winnipeg lab says at least part of the problem behind the out−of−date test stems from the fact that Vietnamese laboratories have had limited success in isolating and growing stocks of the circulating viruses this year. For reasons that are not clear, the virus is not growing well in the cell culture medium that was used in the past, says Darwyn Kobasa, a respiratory−viruses researcher who recently returned from Vietnam.
Source: http://news.yahoo.com/news?tmpl=story&u=/cpress/20050508/ca_pr_on_na/avian_flu_outdated_tests_1

18. *May 07, Los Angeles Daily News* — **Increase of West Nile virus feared.** This season's near−record rainfall in California has spawned fears of a widespread outbreak of potentially deadly West Nile virus and more than a dozen other mosquito−borne viruses, experts said. Researchers at the University of California Davis Center for Vectorborne Diseases said at least 18 mosquito−borne viruses have been detected in California and many of these pose increasing threats to public health. Among these are Western equine, Venezuelan equine encephalitis and St. Louis encephalitis, a historically rural disease that has expanded into the metropolitan Southern California area. "There is always the possibility that new viruses or new vectors will be introduced into California, but in terms of (mosquito−borne viruses) in California, the West Nile virus poses the greatest risk," said Vicki Kramer, head of the Vector Borne Disease Program at the California Department of Health Services. The experts predicted that mosquito−borne illnesses will cause more illnesses and deaths as national and international travel becomes faster and cheaper, commerce proliferates and population centers expand into

new areas.
Source: http://www.contracostatimes.com/mld/cctimes/news/state/11589 347.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

Nothing to report.
[Return to top]

Information Technology and Telecommunications Sector

19. *May 09, Secunia* — **Two vulnerabilities in Mozilla Firefox.** Two vulnerabilities have been discovered in Firefox, which can be exploited by malicious people to conduct cross−site scripting attacks and compromise a user's system. "IFRAME" JavaScript URLs are not properly protected from being executed in context of another URL in the history list. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site. Input passed to the "IconURL" parameter in "InstallTrigger.install()" is not properly verified before being used. This can be exploited to execute arbitrary JavaScript code with escalated privileges via a specially crafted JavaScript URL. A temporary solution has been added to the sites "update.mozilla.org" and "addons.mozilla.org" where requests are redirected to "do−not−add.mozilla.org". This will stop the publicly available exploit code using the two vulnerabilities to execute arbitrary code in the default settings of Firefox.
Source: http://secunia.com/advisories/15292/

20. *May 09, Washington Technology* — **DHS secure network was rushed.** The Department of Homeland Security's (DHS) $337 million network for sharing top−secret data was developed in a rush, and as a result is inadequate and does not meet the needs of its users, according to a new report by the department's Acting Inspector General Richard L. Skinner. Department officials developing the Homeland Security Secure Data Network (HSDN) hurried to finish the job in nine months because they believed they would be cut off from the Pentagon's secure data network by a December 31, 2004 deadline, the inspector general (IG) said. The IG report stated, "…the methods for collecting and documenting the functional and security needs of users during the requirements definition phase for the new network did not provide adequate assurance that user needs at the 600 sites will be met." The 600 sites referred to are DHS intelligence gathering units and federal, state and local agencies involved in homeland security. The inspector general is recommending that all system users be involved in defining its requirements in the future, and that completion of all testing be verified before deployment.
Inspector General's Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/OIG_05−19_Apr05.pdf
Source: http://www.washingtontechnology.com/news/1_1/daily_news/2616 1−1.html

21. *May 09, eWeek* — **University laboratory studies effects of Internet attacks.** A new test laboratory at Iowa State University (ISU) will allow researchers to study how computer networks respond to massive Internet attacks and could lead to breakthroughs in computer defenses and forensics, said a researcher behind the project. The new test network, ISEAGE (Internet Simulation Event and Attack Generation Environment), was funded by a $500,000 grant from the Department of Justice. ISEAGE is the first research lab to be able to re−create any cyber−attack on any part of the Internet infrastructure, said Doug Jacobson, director of information assurance at ISU. The guts of the new test lab are software tools, developed by Jacobson, that let researchers change traffic patterns, replay attacks in endless configurations and collect attack data, Jacobson said. "We can make an attack that looks like it came from 1,000 computers, but we don't need 1,000 computers to do it," he said. The testbed can just as easily simulate attacks from 100,000 Internet−connected machines—or from every Internet address in existence, Jacobson said. Researchers will use ISEAGE to model attacks on critical cyber−infrastructure, such as state and federal computer networks.
Source: http://www.eweek.com/article2/0,1759,1813648,00.asp

22. *May 09, NewScientist* — **Google blackout linked to Internet infrastructure.** A brief blackout at Internet search giant Google has drawn attention to the addressing system that underpins the Web. The Google search page disappeared from view for about 15 minutes late Saturday night, May 7. Some users reported being redirected to an alternative search service called SoGoSearch, but Google has strongly dismissed suggestions that its servers were compromised in any way. Google spokesperson David Krane told the Associated Press that the problem was related to the Domain Name System (DNS), which maps Web names to the numerical Internet Protocol (IP) addresses used by computers. There are thousands of individual DNS servers dotted around the Internet that report back to 13 "root" servers holding master records for DNS mapping. It remains unclear whether the outage at Google was the result of a malfunction in one particular server or the wider system. The outage has drawn attention to widespread reliance of many Web users and services on Google and highlights existing concerns over the stability of DNS infrastructure. In March 2005, the National Academies National Research Council issued a report criticizing the current state of DNS infrastructure.
National Academies' Report: http://www7.nationalacademies.org/cstb/pub_dns.html
Source: http://www.newscientist.com/article.ns?id=dn7357

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: Apple has released a security patch to correct twenty vulnerabilities affecting Mac OS X. These flaws could be exploited by remote or local attackers to execute arbitrary commands, cause a denial of service or obtain elevated privileges.

Current Port Attacks

Top 10 Target Ports	20485 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 135 (epmap), 53 (domain), 41170 (−−−), 139 (netbios−ssn), 6346 (gnutella−svc), 1025 (−−−), 3800 (−−−) 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) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 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