Department of Homeland Security Daily Open Source Infrastructure Report for 16 May 2006

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

Daily Highlights

- The Knoxville Journal Express reports that with over 1,600 mumps cases in the state, the Iowa Department of Public Health and its local public health partners are expanding the ages of Iowans eligible to receive the mumps vaccination. (See item 16)
- The Associated Press reports new X−ray machines that can recognize weapons and explosives and can magnify images of tiny objects have been added at Baltimore's circuit court buildings. (See item 18)
- The Boston Globe reports three New England governors have declared states of emergency as torrential rains flood parts of Massachusetts, New Hampshire, and Maine, washing out roads, flooding basements, and forcing emergency evacuations. (See item 32)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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://www.esisac.com]

1. *May 15, Kyodo (Japan)* — **Japan's power plant security info leaked onto Internet.** Security data on a thermal power plant has been leaked onto the Internet from a virus−infected personal computer, the company in charge of the plant's security said Sunday, May 14. The information was passed onto the Internet through a file−sharing program called Share. The data includes the

locations of various facilities in Chubu Electric Power Co.'s thermal power plant in Owase, Mie Prefecture, including the control room, instrument panel room and boilers, officials of the security company, a Chubu affiliate, said. Also leaked were manuals on how to deal with unconfirmed reports of intruders in the plant, as well as a list of the names and home addresses of the security firm's employees and other personal data on guards, they said. Chubu Power, based in Nagoya, operates five nuclear power reactors in Shizuoka Prefecture.
Source: http://search.japantimes.co.jp/cgi−bin/nn20060515a3.html

[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. *May 15, Consumer Affairs* — **Ohio University's Hudson Health Center network breached.** The news that hackers gained access to the medical data of thousands of Ohio University students, due to a security breach at the university's Hudson Health Center, was only the latest in a series of attacks that have plagued the college since late April. The Hudson Health Center data contained identifying information on 60,000 students, including Social Security and personal identifier numbers, addresses, and data on medical treatments. The Health Center breach followed an attack on a network server containing data on 300,000 Ohio University alumni and donors, including 137,000 Social Security numbers. And on April 21st, the university's Innovation Center was hacked, leading to the exposure of intellectual property files, e−mails, and Social Security numbers. Bill Sams, chief information officer for Ohio University, said that the information was coded in such a way that medical records and personal identifiers could not be immediately matched, reducing the risk to affected individuals. No information was available indicating that the breaches were the work of the same group of hackers.
Source: http://www.consumeraffairs.com/news04/2006/05/ohio_u_data_th eft.html

3. *May 13, Associated Press* — **Glitch causes woes at world's biggest bank.** A computer system glitch caused ATM troubles at the Bank of Tokyo−Mitsubishi UFJ affecting transactions early Saturday, May 13. The troubles included rejected online and ATM transactions for approximately an eight−hour period. The bank said that a hard−disk trouble of the company's host computer may have caused the problem, but the company is still investigating. Kyodo News agency said that the trouble affected some 21,000 ATMs −− 2,000 at bank branches and 19,000 installed at convenience stores −− and the bank received about 3,600 reports in which users said they were unable to withdraw cash.
Source: http://www.wtop.com/?nid=111&sid=790409

4. *May 13, Websense Security Labs* — **Phishing Alert: Republic Bank & Trust.** Websense Security Labs has received reports of a new phishing attack that targets customers of Republic Bank & Trust, which is based in Kentucky. Users receive a spoofed e−mail message, which claims that they have been selected to take a survey for an account credit of $30. This e−mail message contains a link to a phishing Website that prompts the user to enter confidential information after a brief survey.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =485

5. *May 10, Bloomberg* — **Singapore stages anti−terror drill for financial industry.** Singapore staged an emergency exercise for its financial industry to test its response to terrorist attacks. DBS Group Holdings Ltd., Southeast Asia's largest lender, and Citigroup Inc., the biggest U.S. financial services company, were among more than 100 financial institutions that took part in "Exercise Raffles," which included simulated explosions in Singapore's central business district on Tuesday, May 9. The emergency drill was the first such staged in Asia. Terrorist attacks in recent years in the U.S., UK, and in neighboring Indonesia have prompted financial regulators, banks and other institutions in the city−state of 4.3 million people to guard against similar risks. The financial industry, which accounts for about five percent of the workforce, makes up 12 percent of Singapore's $122 billion economy. The mock attacks included explosions at street corners, where banks such as Oversea− Chinese Banking Corp., United Overseas Bank Ltd., and Standard Chartered Plc are located. About 4,000 people participated in the three−and−the−half hour operation. Regulators from Hong Kong, Australia, Malaysia, the Netherlands, Thailand, and Brunei were among observers of the exercise.
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=ap6IhIiS YCuE&refer=asia

[Return to top]

Transportation and Border Security Sector

6. *May 15, Associated Press* — **Transit worker killed by train in Washington, DC.** A transit worker inspecting the subway tracks was killed Sunday, May 14, after being hit by a Metro train, authorities said. Three men were doing routine maintenance work in a tunnel about 100 yards from the south entrance to the Dupont Circle station when the train hit Jong Won Lee, 49, Metro spokesperson Candace Smith said. Investigators from the transit agency as well as the National Transportation Safety Board and the Occupational Safety and Health Administration were trying to determine why he was hit. It is common for workers to be in tunnels when trains are running, Smith said. Lee is the second Metro employee to be killed by a train in the last seven months.
Source: http://www.chron.com/disp/story.mpl/ap/nation/3863053.html

7. *May 15, South Florida Sun−Sentinel* — **Plane touches off hijacking scare in Central Florida.** Looking back on a weekend scare at Orlando Sanford International Airport, officials Sunday, May 14, said all their planning paid off and authorities' response went like clockwork when a small plane sent out an erroneous signal that it had been hijacked. Compounding concern was the plane's veering into restricted airspace over Patrick Air Force Base while the pilot did not answer radio calls. A host of agencies from the FBI and Department of Homeland

Security to law enforcement across Central Florida were involved, and everyone reacted properly, airport President Larry Dale said. The incident started before noon Saturday, May 13, when a rented four−seat Cessna plane took off from the Sanford airport. Planes broadcast a signal so they can be identified on radar. Pilots enter an assigned number when they are in an airport's restricted airspace but use the number 1200 otherwise, Dale said. Either the transponder on the plane malfunctioned or the pilot accidentally entered "7500," sending out a signal that the plane had been hijacked, he said. Police initially closed access to the airport, but Dale said he ordered gates reopened when he learned the plane was flying southeast and was 30 miles from the airport.
Source: http://www.sun−sentinel.com/news/local/florida/orl−plane1506may15,0,7477082.story?coll=sfla−news−florida

8. *May 15, Associated Press* — **Northwest, union impasse heads to court.** Northwest Airlines Corp wants its bankruptcy judge to let it throw out its union contracts with baggage handlers and other ramp workers. A trial on that request began on Monday, May 15, in bankruptcy court in New York. Mediated talks between the International Association of Machinists and the airline last week in Minneapolis quickly fizzled, and there were no new talks over the weekend. Earlier this year 60 percent of those workers rejected Northwest's proposed pay cuts and layoffs, and authorized a strike in case the bankruptcy judge allows Northwest to impose its terms. The union believes a strike by its 5,600 members could shut the airline down. Temporary pay cuts imposed in bankruptcy sliced his hourly wage from $20.20 to $16.35. Some workers feel that the pay cuts and work rule changes Northwest wants won't make the job worth it anymore. Many baggage handlers remain bitter at the airline for 1993 concessions in which they were to be awarded shares in the company. Northwest has said its common stock is likely to be worthless when it exits bankruptcy.
Source: http://www.usatoday.com/travel/flights/2006−05−15−northwest− contracts_x.htm

9. *May 13, Associated Press* — **Northwest Air flight to Hong Kong returns to Tokyo.** A Northwest flight bound for Hong Kong returned safely to Tokyo's international airport at Narita after engine trouble was detected, but no one was injured, an official said Sunday, May 14. Flight No.1, a Boeing 747, developed engine trouble after takeoff Saturday evening and returned safely to Narita about an hour later, causing no injuries, according to airport spokesperson Masaru Motoyama. One of the engines on the right side of the aircraft was malfunctioning, Motoyama said.
Source: http://money.iwon.com/jsp/nw/nwdt_rt_top.jsp?cat=TOPBIZ&src=704&feed=dji&section=news&news_id=dji−00031920060513&date=20060513&alias=/alias/money/cm/nw

[Return to top]

Postal and Shipping Sector

10. *May 14, Associated Press* — **Mercury leak forces evacuation of New Jersey post office.** A mail handler found a package leaking a small amount of mercury in a Swedesboro, NJ, U.S. Postal Service facility Sunday morning, May 14, causing officials to evacuate the building for about three hours, authorities said. The postal worker who found the package was later checked by hazardous materials personnel and permitted, along with co−workers, to re−enter the

building after the leak was cleaned up, said Ray Daiutolo, a regional spokesperson for the postal service.
Source: http://www.courierpostonline.com/apps/pbcs.dll/article?AID=/20060514/NEWS01/60514001/1006

[Return to top]

Agriculture Sector

11. *May 12, Western Farm Press* — **Resistant cavity spot gaining in carrots.** The California carrot industry needs a new weapon to control increasing, tougher strains of cavity spot disease, according to a University of California, Davis, plant pathologist. Mike Davis recently reported on his 2005 research findings during the California Fresh Carrot Advisory Board's research symposium in Bakersfield. He found additional samples of the fungal disease, caused by Pythium species, having resistance to mefenoxam, the active ingredient in Ridomil Gold fungicide, in Kern County. Ridomil Gold is the only chemical control for the pathogen in carrots. Davis said large portions of a few carrot fields, if not entire fields, were recently abandoned because of the disease. "Every year we are discovering more−resistant strains, and when I say more−resistant that means at least 50−fold more insensitive (to Ridomil Gold) than the rest of the Pythium population. We need other materials or strategies to control cavity spot." Cavity spot is shown as horizontal, depressed lesions on mature carrot roots, making them unmarketable. The fungus prefers cool soil temperatures and thrives at 58 degrees.
Source: http://westernfarmpress.com/news/051206−resistant−carrots/

[Return to top]

Food Sector

12. *May 15, Reuters* — **Tuna firms don't have to warn of mercury.** Tuna companies do not have to put labels on their cans warning the fish contains mercury, a San Francisco judge ruled in rebuffing a lawsuit brought by California's attorney general. In a Thursday, May 11, decision, San Francisco Superior Court Judge Robert Dondero ruled against state Attorney General Bill Lockyer, who in 2004 sought to ban the sale of canned tuna without mercury warnings. Lockyer sued Del Monte Foods, maker of StarKist tuna; Bumble Bee Seafoods, a unit of Connors Brothers Income Fund of Canada, maker of Bumble Bee tuna; and Tri−Union Seafoods, maker of Chicken of the Sea tuna. The complaint alleged the firms violated state Proposition 65, an initiative approved by voters in 1986 to require firms to issue warnings before exposing people to "known carcinogens or reproductive toxins."
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006−05−15T121211Z_01_N12193249_RTRIDST_0_HEALTH−FOOD−CALIFORNIA−TUNA−DC.XML&archived=False

13. *May 15, U.S. Department of Agriculture* — **USDA concludes first round of talks on protocol for resumption of U.S. beef sales to China.** A delegation from the U.S. and Chinese governments concluded two days of negotiations to establish a protocol for the resumption of U.S. beef sales to China. "We've made considerable progress with China during these

discussions to reopen their market to U.S. beef and we will meet again soon to conclude the talks," said Under Secretary for Farm and Foreign Agricultural Services J.B. Penn. "We also developed and completed a memorandum of cooperation that provides a basis for addressing food safety issues on an ongoing basis." The discussions in Beijing follow the 17th U.S.−China Joint Commission on Commerce and Trade (JCCT) meeting in Washington last month at which China agreed to reopen its market to U.S. beef with the development of a science−based trading protocol, consistent with World Organization for Animal Health guidelines.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/05/0166.xml

14. *May 15, Central Point News (OR)* — **New Oregon State University research.** In the past, discerning shoppers purchasing "Oregon" strawberries from their grocers' shelves might have ended up with a product that came all the way from Mexico or Central America. And they might have never been made aware of the discrepancy. Now, new testing methods developed by Oregon State University researchers will allow the food industry to determine whether those fresh "Oregon" strawberries came from fields in McMinnville, Burns or the Gulf of Mexico. Fresh produce, coffee and wine are just some of the food products that are often mislabeled −− either unintentionally or on purpose −− and until recently there was not a sure−fire way to determine the true geographic origins of commodities. By looking at stable isotopes and the availability of trace elements in different foods, like that luscious Oregon strawberry, and comparing the results to a database, the researchers can pinpoint within a matter of miles where the berry came from.
Source: http://www.centralpointnews.com/articles/index.cfm?artOID=33 0627&cp=4310

15. *May 12, Animal and Plant Health Inspection Service* — **Wheat exports to Mexico from California resume after ten year ban.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Friday, May 12, announced that wheat shipments from California to Mexico have resumed after a 10−year ban due to Karnal bunt. Mexico banned wheat from the southwestern U.S. after the first detection of Karnal bunt in Arizona in 1996. In June 2005, the U.S. and Mexico agreed to recognize certain wheat−producing areas in California, Arizona, Texas and New Mexico as free of Karnal bunt, with the exception of those areas still regulated by USDA because of the disease. As part of the agreement, the U.S. now recognizes five Mexican states as meeting the requirements for Karnal bunt−free status. Mexico ranks as the United States' third largest foreign market for wheat, setting record−high sales of $459 million in 2004. Karnal bunt is a fungal disease of wheat, durum wheat and triticale, a hybrid of wheat and rye, and is spread primarily through the movement of infected seed.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB/.cmd/ad/.ar/sa.retrievecontent/.c/6_2_1UH/.ce/7_2_5JM/.p/5_2_4TQ/.d/3/_th/J_2_9D/_s.7_0_A/7_0_1OB?PC_7_2_5JM_contentid=2006/05/0162.xml&PC_7_2_5JM_parentnav=LATEST_RELEASES&PC_7_2_5JM_navid=NEWS_RELEASE#7_2_5JM

[Return to top]

Water Sector

Nothing to report.

[Return to top]

Public Health Sector

16. *May 15, Knoxville Journal Express (IA)* — **Mumps vaccine eligibility expands to Iowans 26 through 46 years old.** With over 1,600 mumps cases in the state, the Iowa Department of Public Health and its local public health partners are expanding the ages of Iowans eligible to receive the mumps vaccination. Beginning May 10, Iowans 26 through 46 years old can receive the mumps vaccination from their local health department.
Source: http://www.zwire.com/site/news.cfm?newsid=16640263&BRD=1463&PAG=461&dept_id=180222&rfi=6

17. *May 14, Agence France−Presse* — **One million birds culled in Romania after bird flu outbreak.** Some one million domestic fowl are to be culled in Romania after the H5N1 bird flu virus was found in three locations in the center of the country, Romanian Agriculture Minister Gheorghe Flutur said. "The discovery of bird flu in a farm is a first in Romania, since the first case of the disease was detected on October 7, 2005. We will quickly cull the farm's approximately 350,000 chicken, as well as other poultry in contaminated centers," he said. According to an investigation by the anti−epizootic committee, a farm in Codlea already delivered poultry "illegally" to three counties in central and eastern Romania. Sunday, May 14, veterinary health authorities said they had seized almost three tons of chicken that could be infected by the bird flu virus in a supermarket in the eastern town of Galati.
Source: http://news.yahoo.com/s/afp/20060514/hl_afp/healthfluromania_060514200800;_ylt=Ao2Ho.foh3KIMXFXd.5K4EqJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

18. *May 15, Associated Press* — **New security measures in Baltimore's court buildings.** New security measures are in place at Baltimore's circuit court buildings. New X−ray machines have been added at both buildings. The machines replace a standard metal detector at Courthouse East and an older model X−ray machine at the Clarence Mitchell Courthouse. The machines can recognize weapons and explosives and can magnify images of tiny objects. The courthouses have also added an enhanced "panic button" system. The buttons are located near a judge's bench.
Source: http://wjz.com/topstories/local_story_135080414.html

[Return to top]

Emergency Services Sector

19. *May 15, Government Accountability Office* — **GAO−060−643: Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters (Report).** Hurricane Katrina was one of the largest natural disasters in U.S. history.

Despite a large deployment of resources at all levels, many have regarded the federal response as inadequate. The Government Accountability Office (GAO) has a body of ongoing work that covers the federal government's preparedness and response to hurricanes Katrina and Rita. Due to widespread congressional interest, this review was performed under the Comptroller General's authority. It examined (1) the extent to which pre−Katrina plans and training exercises reflected the military assistance that might be required during a catastrophic, domestic, natural disaster, (2) the military support provided in response to Katrina and factors that affected that response, and (3) the actions the military is taking to address lessons learned from Katrina and to prepare for the next catastrophe. GAO is making recommendations to improve the military response to catastrophic disasters. The recommendations address the needs to clearly delineate military capabilities in the National Response Plan and to improve military plans and exercises. The recommendations specifically address the integration of the military's National Guard and active duty and Reserve forces, as well as response problems associated with damage assessment, communication, search and rescue, and logistics issues. The Department of Defense partially concurred with all of GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06643high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−643

20. *May 14, WCSH−TV (ME)* — **Emergency response put to the test in Maine.** A weeklong maritime exercise in Casco Bay, ME, brought together the Coast Guard, the FBI, and the National Guard from both Maine and New Hampshire, as well as local police and firefighters. The exercise culminated in a drill involving a terrorist arrested on board a Maine fishing boat on Friday, May 12.
Source: http://www.wcsh6.com/home/article.asp?id=35257

21. *May 13, Orlando Sentinel (FL)* — **New generators to supply Florida evacuation artery with emergency electricity.** Eleven new million−watt generators will ensure a full tank, a cup of coffee and an air−conditioned oasis along Florida's evacuation artery this hurricane season. Florida's Turnpike Enterprise officials announced a $7.5 million project Friday, May 12 shortly before one generator, nicknamed "The Boss," started humming with a flip of a switch at Turkey Lake Plaza in Ocoee. That generator and seven more will power eight plazas between Miami and Wildwood during outages. Three others will be used for the Florida Highway Patrol and turnpike operations. The generators will keep restaurants serving, stores selling and gas flowing while residents flee impending storms or work crews arrive after a hurricane hits.
Source: http://www.orlandosentinel.com/news/local/state/orl−turnpike 1306may13,0,5063767.story?coll=orl−news−headlines−state

22. *May 12, Voice Ledger (NY)* — **Drills test New York county's response time.** The distinctive awesome thunder of the C−5A aircraft is a familiar sound to Pleasant Valley, NY, residents. The aircraft regularly soars through Dutchess County skies en route to Stewart Air National Guard Base. The C−5A is one of the largest in the world, wider than a football field and almost as long. It transports tanks, helicopters, and other bulky items. Although there have been few accidents in the craft's nearly 40 year history, the thought of one falling out of the sky is enough to blow anyone's mind. On the morning of Saturday, May 6, local firefighters, emergency personnel, units from the New York Air National Guard, along with state and county police were called upon to respond to just such a calamity. The massive joint planning exercise was the largest of its kind for the county. Dutchess County Executive William Steinhaus was

pleased with the results. "I think the interagency cooperation was very impressive. The turnout of the different agencies is absolutely incredible, and to see the whole incident command structure work the way we designed it should give people in the community a sense of structure," said Steinhaus.
Source: http://www.zwire.com/site/news.cfm?newsid=16624160&BRD=1721&PAG=461&dept_id=72149&rfi=6

23. *May 11, TechWeb* — **Emergency responders can't communicate, Department of Homeland Security warns.** The federal government has given more than $2.1 billion to states for interoperable communications since 2003, but many emergency responders still cannot communicate with each other, Department of Homeland Security Secretary Michael Chertoff warned at a conference in Washington. Chertoff said that a task force of first responders, not representatives from telecommunications companies, would form within two months and begin identifying requirements. "And I want to be very clear about this. It is not up to industry to come to us and tell us what we need. It is up to us to define the requirements that we need for our first responders and then tell industry, here's the solution you've got to come up with," he said. The Department of Homeland Security will set functional requirements and performance standards for the next generation of communications equipment after gaining input from emergency responders. It will also use scorecards to measure performance of departments.
Source: http://www.informationweek.com/news/showArticle.jhtml?articleID=187202331&subSection=All+Stories

[Return to top]

Information Technology and Telecommunications Sector

24. *May 14, Associated Press* — **High definition could choke Internet.** Everyday, it seems, a new service pops up offering to send video over the Internet. While some may be up for it, is the Internet? The answer from the major Internet service providers (ISPs), the telephone and cable companies, is "no." Small clips are fine, but TV−quality and especially high−definition programming could make the Internet choke. Most home Internet use is in brief bursts −− an e−mail here, a Webpage there. If people start watching streaming video like they watch TV −− for hours at a time −− that puts a strain on the Internet that it wasn't designed for, ISPs say, and beefing up the Internet's capacity to prevent that will be expensive. To offset that cost, ISPs want to start charging content providers to ensure delivery of large video files, for example. Internet activists and consumer groups are vehemently against those plans, saying they amount to tilting the Internet's level playing field, one of the things that encourages innovation. They want legislation to guarantee a "neutral" Internet, but prospects appear slim.
Source: http://www.nytimes.com/aponline/technology/AP−Net−Neutrality .html

25. *May 14, Reuters* — **Cyber threats to U.S. business grow more dangerous.** Attacks on U.S. computer networks could escalate from mere inconveniences to disasters that ruin companies or even kill people, according to the head of a cyber−security unit working with the U.S. government. Scott Borg, director of the Cyber Consequences Unit, or CCU, a Department of Homeland Security advisory group, said increasing intelligence "chatter" was pointing to possible criminal or terrorist schemes to destroy physical infrastructure such as power grids. The CCU is considering how to prevent attacks beyond ubiquitous e−mail hoaxes or computer

viruses, with concerns rising about plots to cause power blackouts, tamper with pharmaceutical products or reprogram machinery to build dangerously defective products. Borg's CCU, a small independent unit funded by Homeland Security, spends its time trying to imagine how technology could be used to cripple the United States. It also holds cyber−security exercises for U.S. corporations and investigates reports of attacks on computer systems. A major crisis could be triggered, for instance, by shutting down critical computer systems for as little as four days.
Source: http://www.networkingpipeline.com/showArticle.jhtml?articleI D=187202905

26. *May 12, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−132B: Apple QuickTime Vulnerabilities.** Apple QuickTime contains multiple vulnerabilities. Exploitation of these vulnerabilities could allow a remote attacker to execute arbitrary code or cause a denial−of−service condition. Systems affected: Apple QuickTime on systems running Apple Mac OS X or Microsoft Windows. For more information, please refer to the US−CERT Vulnerability Notes:
VU#289705: http://www.kb.cert.org/vuls/id/289705
Solution: Upgrade to QuickTime 7.1. This and other updates for Mac OS X are available via Apple Update:
http://docs.info.apple.com/article.html?artnum=106704
An attacker may be able to exploit this vulnerability by persuading a user to access a specially crafted file with a Web browser. Disabling QuickTime in your Web browser will defend against this attack vector. For more information, refer to "Securing Your Web Browser":
http://www.us−cert.gov/reading_room/securing_browser/
Source: http://www.uscert.gov/cas/techalerts/TA06−132B.html

27. *May 12, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−132A: Apple Mac Products Affected by Multiple Vulnerabilities.** Apple has released Security Update 2006−003 to correct multiple vulnerabilities affecting Mac OS X, Mac OS X Server, Safari Web browser, Mail, and other products. The most serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Impacts of other vulnerabilities include bypassing security restrictions and denial of service. Systems affected: Apple Mac OS X version 10.3.9 (Panther) and version 10.4.6 (Tiger); Apple Mac OS X Server version 10.3.9 and version 10.4.6; Apple Safari Web browser; Apple Mail. Previous versions of Mac OS X may also be affected. Please see Apple Security Update 2006−003 for further information. Apple Security Update 2006−003 resolves a number of vulnerabilities affecting Mac OS X, OS X Server, Safari Web browser, Mail, and other products. Further details are available in the individual US−CERT Vulnerability Notes:
VU#519473: http://www.kb.cert.org/vuls/id/519473
Solution: Install Apple Security Update 2006−003:
http://docs.info.apple.com/article.html?artnum=303737
This and other updates are available via Apple Update:
http://docs.info.apple.com/article.html?artnum=303737
For additional protection, disable the option to "Open 'safe' files after downloading," as specified in "Securing Your Web Browser":
http://www.us−cert.gov/reading_room/securing_browser/#sgener al
Source: http://www.uscert.gov/cas/techalerts/TA06−132A.html

28.

May 12, BetaNews — **Report: Search engines spread malware.** Security software company, McAfee said Friday, May 12 that the epidemic of spyware and viruses could be linked to search engines. According to research from the company, even seemingly benign search terms could bring up sites loaded with nasty payloads. The study, "The Safety of Internet Search Engines," looked at the five major search engines −− Google, Yahoo, MSN, AOL, and Ask −− and covered a period from January through April. Researchers found that in every search engine, popular keywords returned sites that could be potentially dangerous.
Source: http://www.betanews.com/article/Report_Search_Engines_Spread_Malware/1147449437

29. *May 12, CNET News* — **Oracle to participate in open−source project.** Oracle said it will participate in Grails, an open−source project that seeks to make Java programmers more productive through a close tie−in to the Groovy scripting language. Grails is a project to create a development framework, a set of prewritten software components designed to speed Web−application creation using Groovy. Groovy is designed so programmers can use Java and Groovy within the same development project.
Source: http://news.zdnet.com/2100−9593_22−6071763.html

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 continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 38566 (−−−), 445 (microsoft−ds), 12198 (−−−), 25 (smtp), 41170 (−−−), 6588 (AnalogX), 49200 (−−−), 32459 (−−−) 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

30. *May 16, North County Times (CA)* — **Bomb threat stops plant work for hours.** A bomb threat that apparently was a hoax forced International Rectifier Corp. −− a manufacturer of semiconductors −− to shut down its large plant and evacuate or lock out more than 150 employees from work for several hours Sunday, May 14, officials said. Temecula, CA, police Sgt. Mike Ellsworth said officers received a call notifying them of the threat. Company supervisors evacuated the building and also prevented employees coming to work for the night shift from entering the building, said General Manager Richard Cilla. The police blocked off Business Park Drive at a point just north of the plant to Rancho California Road and dozens of employees waited across Rancho California from the company's property, while its emergency response crew searched the premises.
Source: http://www.nctimes.com/articles/2006/05/15/news/californian/temecula/51406212656.txt

31. *May 14, Associated Press* — **Probe of New York Wal−Mart evacuation focuses on air conditioners.** Authorities said Saturday, May 13's evacuation of a Wal−Mart in Amsterdam (35 miles northwest of Albany, NY), for suspicious fumes may have been caused by an air conditioning problem. Forty people were sickened and 17 of them were treated at a nearby hospital after complaining of itchy eyes, sore throats, and wooziness. The store was open again by 7 p.m. EDT Saturday. Two air conditioners remained turned to be inspected on Monday, May 15, said Kevin Thornton, a Wal−Mart spokesperson.
Source: http://money.iwon.com/jsp/nw/nwdt_rt_top.jsp?cat=TOPBIZ&src=704&feed=dji&section=news&news_id=dji−00024520060514&date=20060514&alias=/alias/money/cm/nw

[Return to top]

General Sector

32. *May 15, Boston Globe* — **A deluge of rain for New England.** Three New England governors declared states of emergency as torrential rains flooded parts of Massachusetts, New Hampshire, and Maine over the weekend, washing out roads, flooding basements, and forcing emergency evacuations. In Massachusetts, members of the National Guard and Red Cross and emergency workers from 20 state and local agencies worked to evacuate people in Peabody and Melrose after sewage backed up into apartment buildings. Five feet of water sloshed over downtown Peabody Sunday afternoon, May 14, rendering useless the sandbags laid out on Saturday. In Melrose, local officials requested boats in case they needed them to help rescue stranded residents, emergency officials said. With river levels rising throughout the region, and rain expected to continue, emergency management officials predicted more flooding over the next several days, especially in Middlesex and Essex counties, the areas already hardest hit. Governor Mitt Romney, overseeing the emergency response from a bunker in Framingham, declared a state of emergency early in the day, activating the National Guard. Governor John Lynch declared a state of emergency in New Hampshire, and Governor John Baldacci of Maine issued a similar order for York County, in the state's southern part.
Source: http://www.boston.com/news/local/massachusetts/articles/2006

/05/15/a_deluge_of_woes_for_region/

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

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.

Department of Homeland Security Disclaimer