Department of Homeland Security Daily Open Source Infrastructure Report
for 17 May 2006

Daily Highlights

- The Department of Transportation has announced the National Strategy to Reduce Congestion on America's Transportation Network, which provides a blueprint for federal, state, and local officials to tackle highway, freight, and aviation congestion. (See item 8)

- The Hawaii Channel reports the Hawaii Department of Transportation is asking for the public's help in tracking down thieves who have been stealing copper wiring −− which is selling for $2.73 to $3 a pound −− from light poles along the H−2 Freeway. (See item 10)

- The Associated Press reports a campground at Utah's Natural Bridges National Monument has been closed because of bubonic plague detected among field mice and chipmunks. (See item 21)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: **Energy**; **Chemical Industry and Hazardous Materials**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation and Border Security**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information Technology and Telecommunications**; **Internet Alert Dashboard**

Other: **Commercial Facilities/Real Estate, Monument &Icons**; **General**; **DHS Daily Report 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://www.esisac.com]

1. *May 15, Reuters* — **Ecuador revokes Occidental oil contract.** Ecuador's Energy Minister, Ivan Rodriguez, said on Monday, May 15, the government would revoke a contract held by Occidental Petroleum and strip the U.S. company of its assets in South America's fifth biggest oil producer. Rodriguez said that Petroecuador had the economic and technical capacity to take

over operations at Occidental's oil fields. Occidental is the country's largest investor and extracts 100,000 barrels of oil per day. The company said Ecuador accounts for about seven percent of its global production and three percent of its proved reserves. While the dispute centered around legal wrangling over a contract, the announcement came amid growing nationalist sentiment in many Latin American countries for more control over energy and mining resources.
Source: http://www.nytimes.com/reuters/business/business−energy−ecua dor.html?_r=1&oref=slogin

2. *May 15, Register−Guard (OR)* — **Safety drills in progress; an OSU lab tests scale models of reactor designs for future viability.** In a nondescript lab building on the Oregon State University (OSU) campus sits a one−quarter−scale working model of a new generation of nuclear power plants, based on what's called a "passively safe" design. It does not have a reactor core and does not generate electricity; instead, water is heated electrically to the same temperature it would reach in a nuclear core. From there, the model acts just like a full−sized version, moving the water along the same pathways and allowing every pump, valve and pipe joint to be subjected to a long script of simulated disasters. The model tests the safety of new reactor designs. OSU has a second scale model built and plans for a third. The model will help to streamline the siting and licensing process for any utility that decides to build one. OSU's scale model uses 80 percent less piping, 50 percent fewer valves and 35 percent fewer pumps than existing nuclear plants. "It's a major simplification of the design, which makes it less expensive, more reliable and safer than previous designs," Reyes said.
Source: http://www.registerguard.com/news/2006/05/15/printable/a1.os unukes.0515.W9OZwv0k.phtml?section=cityregion

3. *May 15, MarketWatch* — **Electric industry readies reliability standards.** Mandatory reliability standards for the electricity industry, as required by the Energy Policy Act in 2005, are expected to be in place ahead of next summer, more than three years after blackouts shut down major portions of the U.S. power system. The industry believes it can have the reliability rules in place "well before the summer of 2007," said Rick Sergel of the North American Electric Reliability Council (NERC), at a hearing before the Senate Energy and Natural Resources Committee on Monday, May 15. The Federal Energy Regulatory Commission (FERC) is reviewing NERC's application to become the Electric Reliability Organization, the organization that will oversee the reliability rules. Discussions continue over how much deference regions of the country should be given to impose region−specific requirements on power grid operators and users. Sergel said some regional difference may be necessary to reflect physical differences in electricity infrastructure. Debate has also ensued over who will be required to comply with the rules. NERC plans to compile a registry of all owners, operators, and end users whose actions or inactions can have a material impact on the reliability of the bulk power system.
NERC testimony:
ftp://www.nerc.com/pub/sys/all_updl/docs/testimony/Sergel−%20testimony0515.pdf
FERC testimony: http://www.ferc.gov/EventCalendar/Files/20060515151838−SENR% 20EPAct%2005%20Electric%20Reliability%20Provisions%20(Moot)%_2005−15−06.pdf
Source: http://www.marketwatch.com/News/Story/Story.aspx?guid=%7B827 2BEEA−DB72−4956−843D−212CC0C14446%7D&siteid=google

Chemical Industry and Hazardous Materials Sector

Nothing to report.

Defense Industrial Base Sector

Nothing to report.

Banking and Finance Sector

4. *May 16, SmartPros* — **AICPA loses hard drive with member data.** The American Institute of CPAs (AICPA) sent a letter to its 330,000 members notifying them that a computer hard disk containing their personal information, including Social Security numbers, has been lost in transport. Sent on Monday, May 8, the letter explains that "the hard drive was damaged and had been sent out for repair by an employee in direct violation of the Institute's internal control policies and procedures." The hard drive contained names, addresses, and Social Security numbers of AICPA members −− but not credit card information. The AICPA said there is no evidence that the information has been inappropriately accessed. A search with FedEx Express did not find the drive, leading the institute to believe this "a case of a package being lost." Source: http://accounting.pro2net.com/x52999.xml

5. *May 16, MIT Tech* — **MIT discovers personal data leak.** Personal records, including some social security numbers, of approximately 800 members of the Massachusetts Institute of Technology (MIT) community were recently e−mailed to an MIT mailing list, according to an MIT press release. The file containing the information was sent from the office of the vice president for research, and was received by approximately 150 people, most of whom are affiliated with MIT. MIT became aware of the incident on Wednesday, April 26. Timothy J. McGovern, information technology security support manager, said that everyone whose personal information had been compromised has been notified. He also said that the people who accidentally received the e−mail have been "100 percent" cooperative. Part of the purpose of dialogue between the university and the recipients of the e−mail has been to determine whether they had looked at or forwarded any of the personal data, McGovern said. A task group is being formed in direct response to the security leak, he said. Source: http://www−tech.mit.edu/V126/N26/26security.html

6. *May 15, Wireless Week* — **County slaps warning label on Wi−Fi.** A new law in New York, set to become effective this October, would make local businesses providing broadband wireless access in Westchester County install basic firewall technology for their customers' protection and post signs where the network is available, warning consumers about the possible danger using a wireless network poses to computer users. The law would apply to networks that store customer credit card information and businesses that have Internet−related revenue above $300 per year that provide the networks, says Scott Fernqvist, special assistant to the county's

3

chief information officer. The revenue threshold is to avoid making homeowners with in–home Wi–Fi networks comply, he explains. The law is aimed at protecting users from skyrocketing identity and electronic information theft, he says. The law is the first of its kind, according county officials who note that they have received inquiries from cities across the globe –– from South Korea to Great Britain to Czechoslovakia. Westchester County drew up the rules primarily with retailer–supplied Wi–Fi networks, such as those supplied by hotels and coffee shops, in mind, Fernqvist says. Their use and increasing identity and information theft make for a possibly dangerous combination.
Source: http://www.wirelessweek.com/index.asp?layout=articlePrint&ar ticleID=CA6334959

7. *May 15, CNET News* — **Credit card security rules to get update.** Proposed new security rules for credit card–accepting businesses will put more scrutiny on software, but let them off the hook on encryption. The update to the Payment Card Industry (PCI) Data Security Standard, due this summer, responds to evolving attacks as well as to challenges some businesses have with the encryption of consumer data, said Tom Maxwell of MasterCard International. The proposed update includes a requirement to, by mid–2008, scan payment software for vulnerabilities. Currently, merchants are required to validate only that there are no security holes in their network. Another proposed change to the security rules may hurt security of consumer data, critics said. The new version of PCI will offer merchants more alternatives to encryption as a way to secure consumer data. "Today, the requirement is to make all information unreadable wherever it is stored," Maxwell said. But this encryption requirement is causing so much trouble for merchants that credit card companies are having trouble dealing with requests for alternative measures, he said. In response, changes to PCI will let companies replace encryption with other types of security technology, such as additional firewalls and access controls, Maxwell said.
Source: http://news.com.com/Credit+card+security+rules+to+get+update /2100–1029_3–6072594.html?tag=cd.top

[Return to top]

Transportation and Border Security Sector

8. *May 16, Department of Transportation* — **National initiative to tackle highway, freight, and aviation congestion.** Calling congestion one of the single largest threats to the economy, Department of Transportation Secretary Norman Y. Mineta on Tuesday, May 16, announced a new national initiative to tackle highway, freight, and aviation congestion. He noted that America loses an estimated $200 billion a year due to freight bottlenecks and delayed deliveries. The Secretary added that consumers lose 3.7 billion hours and 2.3 billion gallons of fuel sitting in traffic jams and that airline delays waste $9.4 billion a year. The new initiative, the National Strategy to Reduce Congestion on America's Transportation Network, provides a blueprint for federal, state and local officials to tackle congestion, Mineta said. He noted that over the coming months, the Department of Transportation will focus its resources, funding, staff and technology to cut traffic jams, relieve freight bottlenecks and reduce flight delays. The Secretary also announced that he would convene the Surface Transportation Policy and Revenue Commission for its first meeting on Wednesday, May 24th. He said he would task the commission with finding solutions that not only raise revenue for highway and transit projects, but also reduce the cost of congestion by focusing more on system performance.

The initiative: http://isddc.dot.gov/OLPFiles/OST/012988.pdf
Secretary's remarks: http://www.dot.gov/affairs/minetasp051606.htm.
Source: http://www.dot.gov/affairs/dot5706.htm

9. *May 16, Reuters* — **Lufthansa jumbo jet collapses on nose at Frankfurt.** A Lufthansa AG jumbo jet collapsed on its nose at Frankfurt airport when the front landing gear gave way as it was preparing to fly to New Delhi, an airline spokesperson said Monday, May 15. The 242 passengers and 16 crewmembers on board the Boeing 747–400 had to abandon the plane after the nose sank down onto a waiting tow truck. "The cause of the fall is not yet known. It's very unusual," said an airline spokesperson. The plane was relatively new and had been delivered to Lufthansa in December 2001.
Source: http://www.usatoday.com/travel/flights/2006–05–16–lufthansa– jet_x.htm

10. *May 16, Hawaii Channel* — **Wire thefts cause freeway light outages.** The Hawaii Department of Transportation is asking for the public's help in tracking down thieves who have been stealing copper wiring from light poles along the H–2 Freeway. Thieves have struck three times in six months. Drivers along a stretch of the H–2 Freeway near the Ka Uka Avenue overpass are in the dark at night after vandals have ripped off the copper wires from the light posts in the area. The first time it happened was in October. They hit again in December. In the last few weeks, the culprits hit again. It's creating a dangerous situation and costing taxpayers thousands of dollars. About 50 light poles along about a quarter–mile of the H–2 Freeway are not lit up at night after being stripped of their copper wiring. "That creates a driving problem or driving hazard because this area doesn't have any town lights to light it up," said Hawaii Department of Transportation Director Rod Haraga. Stealing copper wiring can be a lucrative business. Copper sells for between $2.73 and $3 a pound on the market.
Source: http://www.thehawaiichannel.com/news/9210060/detail.html

11. *May 16, CNN* — **Coast Guard hunts for missing cruise ship passenger.** The U.S. Coast Guard began searching Tuesday, May 16, for a 21–year–old man believed to have fallen from a cruise ship sailing from Port Canaveral, FL, to the Bahamas, a Coast Guard spokesperson said. Daniel Dipiero of Augusta, OH, was reported missing Monday morning, May 15, from the Royal Caribbean International's Mariner of the Seas cruise liner, but ship officials did not alert the Coast Guard until eight hours later, said Coast Guard Petty Officer Ryan Doss. In a written statement, the company said, "a variety of onboard announcements and searches were carried out Monday."
Source: http://www.cnn.com/2006/US/05/16/man.overboard/

12. *May 16, Fort Madison Daily Democrat (IA)* — **Coal train derails, leaving cars in yard.** According to Burlington Northern Santa Fe (BNSF) officials, 16 out of 22 cars, each carrying a ton of coal, turned over when the westbound train derailed about 2 a.m. CDT on Friday, May 12, in Donnellson, IA. The train, which was traveling to the St. Louis area, came from the Powder River basin area in Wyoming. No injuries were reported as a result of the incident. BNSF officials say the derailment is still under investigation and they still do not have a damage estimate.
Source: http://www.dailydem.com/articles/2006/05/16/news/news1.txt

[Return to top]

Postal and Shipping Sector

13. *May 16, DMNews* — **USPS, Washington Mutual temporarily suspend NSA proceeding.** Washington Mutual Bank and the U.S. Postal Service (USPS) have temporarily suspended their Negotiated Service Agreement (NSA) proceedings until May 25, according to a document filed with the Postal Rate Commission on Monday, May 15. On March 29, the USPS filed a NSA with Washington Mutual Bank based on encouraging the company to increase its use of First Class mail. The USPS sought a three−year agreement with Washington Mutual covering First−Class Mail for the bank's credit card services. An NSA is a contract between the postal service and a company, providing customized pricing incentives based on the company's mail operations. The changes in rates and mail classification needed to implement the NSA require review and recommendation by the Postal Rate Commission and then approval by the USPS Board of Governors Washington Mutual would get declining block rates for mailing volumes above certain thresholds of First Class Mail relating to the company's credit card products and credit services, the filing said. The USPS estimated it would benefit by $46.3 million over the life of the NSA.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3690 2

[Return to top]

Agriculture Sector

14. *May 16, Evening Sun Reporter (PA)* — **State begins plum pox testing.** State and federal agriculture officials will begin surveying and testing Pennsylvania stone fruit trees Tuesday, May 16, as part of a plum pox virus eradication program. Karl Valley of the Pennsylvania Department of Agriculture said that a majority of the plum pox testing will take place in Adams, Cumberland, Franklin and York counties, since those are the areas where infected fruit has been found in recent years. Five plum pox−infected trees were found in 2005 of the 269,000 samples taken throughout the state. All five of the infected trees were found in Menallen Township. Those trees were destroyed as well as 120 acres of stone fruit trees within 500 meters of them.
Plum pox virus information: http://sharka.cas.psu.edu/
Source: http://www.eveningsun.com/localnews/ci_3828931

15. *May 16, Nature Conservancy* — **Effort to restore native oysters in Chesapeake Bay.** The Nature Conservancy's Chesapeake Bay Initiative, a multi−state effort, announced the launch of its first native oyster restoration project in the Chesapeake Bay watershed. The Conservancy and the Chesapeake Bay Foundation (CBF) are collaborating on the project, which received funding through a national partnership between the Conservancy and the National Oceanic and Atmospheric Administration's Community−based Restoration Program. The Conservancy selected the Piankatank River because of its unusual gyre−like Native oysters from the CBF farm. Volunteers, partners and staff spread oysters along the reef in the Piankatank River.
Source: http://www.nature.org/wherewework/northamerica/states/maryland/press/press2438.html

16. *May 16, Associated Press* — **Whirling disease appears in another Utah stream.** A disease that can deform trout and eventually lead to their starvation continues to spread swiftly through Utah's waterways. The Utah Division of Wildlife Resources (DWR) announced that six of 60 brown trout taken from Huntington Creek last fall were found to have whirling disease. Huntington Creek is a blue–ribbon fishery. The designation means the creek has a viable population of wild fish. The discovery of whirling disease in Huntington Creek was not a surprise, but it illustrates how quickly and easily the disease can spread. Last year, officials at the DWR's Fisheries Experiment Station in Logan found fish infected with the disease in Huntington Creek's tributaries. The DWR is asking anglers and others to slow the spread of whirling disease by disinfecting boats, trailers, waders, boots and float tubes before transporting them to a new body of water. Utah fisheries carrying whirling disease have shown little ill effect on wild populations. But the trout malady has cost millions of dollars at three state hatcheries that tested positive and had to be shut down for lengthy decontamination periods. Thousands of pounds of trout were destroyed, reducing the number of fish available to anglers. Whirling disease information: http://www.protectyourwaters.com/hitchhikers/others_whirling _disease.php
Source: http://www.jacksonholestartrib.com/articles/2006/05/16/news/ regional/4094571afeaa2c3a8725716f00787749.txt

17. *May 15, iBerkshires (MA)* — **Wasting disease undetected in Massachusetts deer.** No evidence of chronic wasting disease (CWD) was detected in Massachusetts deer based on data gathered during the 2005 hunting season. Results from a federally certified veterinary diagnostic laboratory indicate that all the deer brain, lymph node, and tonsil samples taken during last fall's hunting season tested negative for the disease. During the fall 2005 deer hunting season, 577 samples were collected from hunter–harvested, road–killed and targeted deer across the state for CWD testing. This was the fourth year of sampling in Massachusetts as part of a nationwide CWD monitoring and surveillance program.
CWD information: http://www.cwd–info.org
Source: http://www.iberkshires.com/story.php?story_id=19905

18. *May 14, Oroville Mercury Register (CA)* — **Almond crop damage less than feared.** Despite early predictions of extensive crop damage, the almond subjective report shows a billion–pound forecast for California, up 12 percent from last year's estimate at this time. Almonds reached the billion–pound mark for the 2002–2003 season, which the industry wants to sustain to continue to provide almonds to new markets that have been created in recent years. In early March growers were pessimistic after a blast of spring like weather encouraged the blooms on early almond varieties. Then frost broke out. Next was icy rain and high winds. There was also concern about lack of pollination due to disease that has harmed bee colonies. But this also proved not to be the major setback some had feared. The subjective is generated by experienced farmers going out and reporting their best estimate of how the crop will shape up.
Source: http://www.orovillemr.com/news/chico/ci_3821464

[Return to top]

Food Sector

19. *May 16, USA Today* — **Japan wants answers on U.S. beef.** Japan wants to see the results of a survey of U.S. meatpacking plants before starting talks on reopening its market to American beef, Japan's agriculture minister said Tuesday, May 16. Japan banned U.S. meat in January over worries about mad cow disease, and U.S. officials are in Tokyo this week to restart talks on lifting the ban. Agriculture Minister Shoichi Nakagawa said the negotiations could start as soon as Wednesday, May 17, if Tokyo gets the answers to questions it had about 37 meatpacking plants. "We only received an overview but there are things we want to confirm," Nakagawa told reporters. "We want to hold talks once we receive answers."
Source: http://www.usatoday.com/news/health/2006−05−16−japan−us−beef_x.htm

[Return to top]

Water Sector

20. *May 15, Associated Press* — **Heavy rains undermining sewage treatment.** Massachusetts residents already deluged by historic rainfalls faced a second problem Monday, May 15, as wastewater treatment plants along the Merrimack River started to fail, dumping raw sewage that threatened to contaminate passers−by and fishing areas. In Haverhill, a 42−inch main carrying wastewater to a treatment plant broke Sunday, May 14, sending sewage into the Merrimack at a rate of 35 million gallons a day. Governor Mitt Romney said a permanent repair will require replacement of about two miles of line, with the work being done by crews from as far away as New Jersey. Romney also said that just upstream in Lawrence, a regional wastewater treatment plant serving the city, Andover, North Andover, and Salem, NH, was at risk of being shut down because floodwaters were threatening its power plant. That could spill an additional 115 million gallons per day of untreated wastewater into the river. And in Lowell flood waters threatened the city's drinking water treatment plant. The governor said the city had a 24−hour reserve and was exploring alternate supplies from neighboring communities.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/05/15/heavy_rains_pack_a_second_punch_undermining_sewage_tr eatment/

[Return to top]

Public Health Sector

21. *May 16, Associated Press* — **Utah campground closed because of plague in rodents.** A campground at Natural Bridges National Monument has been closed because of bubonic plague detected among field mice and chipmunks. Plague also has been found this spring in rodent populations at Mesa Verde National Park and Colorado National Monument. National Park Service officials said there never has been a reported human case of bubonic plague originating from the parks or national monuments. Several weeks ago, park rangers noticed a large number of dead field mice at Natural Bridges. Chief Ranger Ralph Jones showed that tests indicated they died from the plague. Plague occurs throughout the West, but is concentrated in the Four Corners area of Utah, Colorado, New Mexico and Arizona.
Bubonic plague information: http://www.bt.cdc.gov/agent/plague/
Source: http://hosted.ap.org/dynamic/stories/C/CAMPGROUND_CLOSED_PLA GUE?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2006−05−16−0

22. *May 16, Agence France−Presse* — **Possible case of human case of bird flu in Romania.** A young Romanian woman showing bird flu−like symptoms was admitted to the contagious diseases hospital in Bucharest, the hospital's director Adrian Streinu−Cercel said. The 25−year−old woman "has respiratory problems and comes from Sita Buzaului," a village in central Romania where bird flu is suspected, according to preliminary tests, Streinu−Cercel said. Romanian health authorities were on the hunt for several dozen tons of chicken product produced at a site where bird flu had been found, triggering fear among consumers. The H5N1 strain of the flu was found at a farm in Codlea in central Romania and may have contaminated chicken products shipped to supermarkets.
Source: http://news.yahoo.com/s/afp/20060516/hl_afp/healthfluromania human_060516110726;_ylt=AutQ8Y2o7DdqKu2Hn0F6ipmJOrgF;_ylu=X3 oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[[Return to top](#)]

Government Sector

Nothing to report.
[[Return to top](#)]

Emergency Services Sector

23. *May 16, WZRB−TV (LA)* — **Panel approves emergency communication bill.** On Monday, May 15, a Louisiana state House committee approved a plan that would rely on text messages, e−mails and message boards to keep the public informed during emergencies, but it can't be put into place before June 1. During Hurricanes Katrina and Rita, many cell phone towers lost power or were damaged by wind, and the ones left standing were so overloaded that text messages became one of the best ways to communicate. That's why lawmakers want to allow the state to send residents messages with the latest emergency information.
Source: http://www.2theadvocate.com/news/2807481.html

24. *May 14, Portsmouth Herald (NH)* — **Drill trains emergency workers for a mass−casualty accident.** A man hijacked a Boeing 727 carrying about 100 passengers. The terrorist then set off a bomb that wounded at least half of those on the plane. This scenario was part of a drill on Saturday, May 13, at the Pease International Airport in Portsmouth, NH. About 100 volunteers and almost as many firefighters and emergency workers were part of Seacoast Response 2006, a full−scale exercise to prepare for any type of emergency involving numerous injuries or casualties. Assistant Portsmouth Fire Chief Steve Achilles said it took emergency personnel only a minute to sort the injured from the non−injured and then categorize the injured by level of severity before determining which ones needed to go to the hospital. Overall, he said, it was a success. He said, however, that he would have liked to see it take less time to get patients into ambulances.
Source: http://www.seacoastonline.com/news/05142006/news/102697.htm

Information Technology and Telecommunications Sector

25. *May 15, Reuters* — **Web search sites give new ways to find results.** For information seekers, the days of culling Web search pages, ten machine−generated hyperlinks at a time, may be numbered. On Monday, May 15, Yahoo Inc. took the next step to realize its vision of combining human advice with machine automation to offer more relevant ways of searching the Web. It is using the millions of human suggestions from its recently introduced Yahoo Answers to complement the mathematically organized features of its core search system. "It's the right time now to augment Web search results with some human touch," said Tim Mayer, Yahoo's product manager for Web search. "We are making search better by allowing users to tap into the collective knowledge of other people." Meanwhile, Bill Gross, the inventor of paid Web search who sold the system to Yahoo, is set to unveil a new version of his latest project. Snap.com is aimed at broadband users and gives people visual snapshots of Websites before they click. These innovations in how to search for information on the Web aim to compete with the dominant search provider, Google Inc., which analysts say still has a big lead in the current generation of Web search technology.
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=187203011

26. *May 15, TechWeb News* — **Keyloggers, spyware continue to strike enterprises.** Nearly one in five enterprises have had workers' PCs infected with keyloggers, the worst kind of spyware, a survey released Monday, May 15 said. Keyloggers are a type of spyware, and are used to record keystrokes (and sometimes mouse movements as well) to capture information such as usernames and passwords. They're often planted on consumers' PCs by identity thieves, but are becoming a corporate problem, too. The poll, conducted by Harris Interactive for San Diego−based security vendor Websense, found that 17 percent of IT administrators said that one or more employees had launched a keylogger on their network. In last year's survey, only 12 percent of administrators had acknowledged that keyloggers infected their domains. Bots are also a major problem for corporations, as they are for consumers, the survey showed. Just over a third of administrators (34 percent) were confident that they could keep bots from infecting workers' PCs when those machines weren't connected to the company's network, while almost one in five (19 percent) said that they have had employees' work desktops or laptops hit by a bot.
Source: http://www.techweb.com/article/printableArticle.jhtml;jsessi onid=NYTZFP2AMAGYQQSNDBGCKHSCJUMEKJVN?articleID=187203291&si te_section=700028

27. *May 15, Security Focus* — **Sun Java applet Font.createFont remote denial−of−service vulnerability.** Sun Java is prone to a remote denial−of−service vulnerability. This issue is due to a failure in the application to properly handle certain Java applets. Successfully exploiting this issue will cause the application to create a temporary file that will grow in an unbounded fashion, consuming all available disk space. This will result in a denial−of−service condition. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17981/info
Solution: http://www.securityfocus.com/bid/17981/solution
Source: http://www.securityfocus.com/bid/17981/discuss

28. *May 12, Network World* — **Open−source management arrives.** Six open−source companies and project sponsors founded an industry organization to elevate the status of open−source management tools in enterprise IT shops. The Open Management Consortium (OMC) says it will develop standards to simplify the job of integrating disparate open−source management applications in an effort to make managing large enterprise networks with open−source tools easier for users. Most companies use several management tools, but the majority of proprietary products available today require extensive integration for them to share data −− even when they're from the same vendor. The OMC proposes its members develop common methods of collecting, sharing and reporting on management data collected across enterprise networks. Vendors such as Centeris, GroundWork Open Source, Hyperic and Splunk have already started to open parts of their proprietary software code and make it available through open source licenses. They separately emerged in the past year and straddled the open source and proprietary worlds, offering management applications rooted in open source and in some cases, providing free versions for download.
Source: http://www.networkworld.com/news/2006/051206−open−source−man agement.html?page=1

29. *May 10, Security Focus* — **Symantec Enterprise Firewall / Gateway Security HTTP proxy internal IP leakage weakness.** Symantec Enterprise Firewall and Gateway Security products are prone to an information disclosure weakness. A request of the form "get/XX HTTP/1.0" (note the missing space) triggers the exposure. The firewall seems to forward the request and to wait a certain time for a reply from the Webserver, until the timeout is reached.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/17936/info
Solution: http://www.securityfocus.com/bid/17936/solution
Source: http://www.securityfocus.com/bid/17936/discuss

Internet Alert Dashboard

Upgrade there software to Apple QuickTime 7.1:
http://www.apple.com/support/downloads/quicktime71.html

Disable QuickTime in your web browser to prevent attackers from exploiting this vulnerability by persuading a user to access a specially crafted file with a web browser.

Note: Disabling QuickTime in your web browser will defend against this attack vector.

For more information please review:

Securing Your Web Browser document:
http://www.us−cert.gov/reading_room/securing_browser/

Standalone Apple QuickTime Player:
http://www.apple.com/quicktime/download/standalone.html

Mac OS X: Updating your software:
http://docs.info.apple.com/article.html?artnum=106704

VU#570689 Apple QuickTime FlashPix integer overflow:
http://www.kb.cert.org/vuls/id/570689

VU#289705 Apple Quicktime JPEG integer overflow:
http://www.kb.cert.org/vuls/id/289705

We will continue to update current activity as more information becomes available.

PHISHING SCAMS

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.

[[Return to top]]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[[Return to top]]

General Sector

30. *May 16, Associated Press* — **Portions of New England submerged in water.** Across northeastern Massachusetts, thousands of people fled submerged neighborhoods during the region's worst flooding in nearly seven decades. More than a foot of rain fell during the weekend in some areas. The storms have swamped much of northern New England. In New Hampshire, more than 600 roads were damaged, destroyed or under water. In Maine, flooding washed out dozens of roads and bridges, and threatened a pair of dams along the swollen Salmon Falls River in Lebanon. Two areas of Lebanon near the Spaulding Dam were evacuated Monday as a precaution. In Lowell, MA, crews took to the streets in boats and used bullhorns to urge 1,000 households to evacuate. Several hundred Methuen, MA, residents, who live downstream of the Spicket River Dam, left their homes after officials became concerned that the dam, shored up by several thousand sand bags, would give way under the pressure of the raging river. Schools across the North Shore and Merrimack Valley as well as in southern New Hampshire stayed closed Tuesday.
Source: http://www.usatoday.com/weather/storms/2006−05−14−new−englan d−flooding_x.htm

[[Return to top]]

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.

<u>Department of Homeland Security Disclaimer</u>

The DHS 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.