Department of Homeland Security Daily Open Source Infrastructure Report for 01 May 2006

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

Daily Highlights

- An intruder gained access to a Defense Department computer server and compromised confidential health care insurance information for more than 14,000 people under the TRICARE system, the Associated Press reports. (See item 10)
- The Department of Homeland Security announced Friday, April 28, the release of the Maritime Infrastructure Recovery Plan, one of eight plans supporting the National Strategy for Maritime Security. Key elements of the plan include guidelines for coordinated, national−level efforts to restore the flow of cargo and passenger vessels in response to a major disruption to the maritime transportation system. (See item 17)

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 01, Associated Press* — **Iraq oil output lowest since invasion.** With oil prices above $70 a barrel fouling the world economy, dismay is focusing on Iraq, whose exports have slipped to their lowest levels since the 2003 invasion. Iraq's oil production has slipped further and further since the invasion, to an average of two million barrels a day. It has never regained the reduced production levels that prevailed in the 1990s, when Iraq was under tough U.N. sanctions. Iraq is not covering its own needs. The rickety Iraqi oil system has been damaged repeatedly by insurgent sabotage and attacks on maintenance crews. Corruption, theft of oil, and widespread

mismanagement compound the problems, analysts say. Iraq also lacks laws that would protect foreign investment, and its government is still sorting out whether oil will be controlled by the central government or the provinces. The result: Iraq is importing refined oil products at record high prices at a time that it should be boosting exports to take advantage of those prices to earn money for reconstruction. In 2005, Iraq's exports averaged just 1.4 million barrels a day. This winter proved disastrous, with January exports failing to reach even one million barrels a day, said George Orwel of Petroleum Intelligence Weekly.
Source: http://abcnews.go.com/International/print?id=1902718

2. *April 30, Associated Press* — **Vermont Yankee power boost stopped again.** The Vermont Yankee nuclear plant had to stop short of its goal of increasing its power by 20 percent when two new problems cropped up at the plant Friday, April 28. Plant spokesperson Robert Williams said the reactor was running into a problem that twice before in recent weeks has prompted it to halt the "power ascension" process. The problems are acoustic signals from gauges that are picking up what may be new strains on the plant's steam dryer. The Nuclear Regulatory Commission said later that a second problem possibly involving the steam dryer also showed up Friday. The steam dryer has been a source of problems at other nuclear plants around the country that have increased their power output. It is a large component at the top of the reactor that removes moisture from steam made by the reactor before it is sent to the turbines that spin to generate electricity. NRC spokesperson Neil Sheehan said the plant determined on Friday that too much moisture was being allowed to go to the turbines. Diane Screnci of NRC's Northeast regional office, said the cause of the excessive moisture would not be known until after engineering studies are done.
Source: http://www.wcax.com/Global/story.asp?S=4835095&nav=menu183_1_0

3. *April 29, Philadelphia Inquirer* — **FERC approves LNG plant.** BP got a major boost in its plans to build a liquefied natural gas import terminal in Gloucester County, PA, Friday, April 28, when the Federal Energy Regulatory Commission (FERC) recommended the project go forward. The plan still requires full approval from the commission. BP announced plans in December 2003 to build a $600 million terminal in Logan Township that would import enough liquefied natural gas (LNG) to serve five million homes and meet a rising demand for the fuel. But the proposal has generated a fierce debate about potential terrorism risks and has stoked a border war between New Jersey and Delaware. The project remains in litigation now before the U.S. Supreme Court. The consequences of a terrorist attack on an LNG tanker are unknown. Sandia National Laboratories has reported that such an attack could create a fire hot enough to cause second−degree burns on people a mile away and damage to buildings within a third of a mile. Industry representatives say that LNG has an excellent 40−year safety record and that releases are extremely unlikely. BP has said the terminal would be outfitted with numerous safety devices.
Source: http://www.macon.com/mld/inquirer/news/local/14456751.htm?source=rss&channel=inquirer_local

4. *April 29, Houston Chronicle* — **Port Arthur expansion would more than double refinery's output.** Oil refiner Motiva Enterprises confirmed Friday, April 28, that a $3.5 billion−plus expansion of its Port Arthur refinery is on track. The project would make the refinery the nation's largest, Motiva said. The Port Arthur expansion would increase capacity at the plant by 325,000 barrels per day. Currently, the refinery can process 285,000 barrels of crude per day.

William Welte, Motiva's president and chief executive officer, said: "Adding 325,000 barrels per day of refining capacity would be the equivalent of building a new refinery in the United States...We are taking deliberate steps to strengthen our nation's ability to meet future demand for gasoline, diesel and aviation fuels." Motiva, which owns refineries, a distribution system, and a marketing network, is owned by Saudi Refining and Shell. Pending regulatory approvals, Motiva said it expects to start final engineering work later this year and could begin construction in 2007. The expansion would come on line in 2010. The expansion would bring much−needed supplies of transportation fuel to the market, according to Motiva, particularly in the eastern and southern regions of the country.
Source: http://www.chron.com/disp/story.mpl/business/3828560.html

5. *April 29, Bay News 9 (FL)* — **Electricity theft growing.** Electricity theft is becoming a growing problem in the Tampa Bay, FL, area. While Tampa Electric Company (TECO) officials won't say how electricity is being stolen, they said they are seeing more people figuring out how to turn on lights and raising electric garage doors illegally. TECO investigator George Cermeno said: "We're constantly fighting battles in the field...We get new cases reported to us daily." People who get caught will have to pay for all the power they stole plus the cost for the investigation itself. TECO officials estimate that 15 to 18 percent of everyone's power bill is making up for the amount of electricity stolen every day.
Source: http://www.baynews9.com/content/36/2006/4/29/156313.html

6. *April 26, Associated Press* — **PDVSA to build oil upgrading refinery.** State oil company Petroleos de Venezuela SA (PDVSA) will build a heavy oil upgrading refinery in the country's oil−rich Orinoco River basin, the government news agency said. PDVSA aims to upgrade 800,000 barrels a day of heavy crude, the Bolivarian News Agency quoted Alejandro Granado, the head of refining at PDVSA, as saying Tuesday, April 25. The plan is part of a larger effort by Venezuela to boost refining operations to exploit the vast potential of its Orinoco tar belt. The area holds enormous deposits of extra−heavy oil and tar−like bitumen, which were long considered economically inefficient to produce. But recent technological advances have changed that. Currently, BP, Exxon Mobil, Chevron, ConocoPhillips, France's Total SA, and Norway's Statoil ASA are operating four upgrading projects. The Venezuelan government believes some 235 billion barrels of crude are recoverable from the Orinoco region. If that claim is established, it would give Venezuela the world's largest crude oil reserves.
Source: http://biz.yahoo.com/ap/060426/venezuela_oil.html?.v=2

7. *April 26, ISO New England* — **ISO New England forecasts possible record−breaking electricity demand for summer 2006.** ISO New England Inc., the operator of the region’s bulk power system and wholesale electricity markets, on Wednesday, April 26, issued its summer 2006 electricity demand outlook. Summer electricity use for New England is forecast to reach 27,025 megawatts (MW) on at least one day this summer under normal weather conditions of about 90 degrees Fahrenheit. Extreme weather conditions, such as an extended heat wave of approximately 95 degrees Fahrenheit, could increase peak demand for electricity by 1,760 MW. Stephen G. Whitley, ISO New England’s Senior Vice President and Chief Operating Officer said: “New England should have sufficient electric generation to meet demand this summer...However, the region or local areas could experience tight supply situations if generation is constrained or if hot and humid weather increases demand. In these cases, the ISO has a series of longstanding measures to maintain reliability by keeping electricity supply and

demand in balance." Whitley added: "While demand for electricity continues to grow across New England, construction of new generating resources has stagnated. Without new investment in power infrastructure and greater energy efficiency and conservation, New England could soon be consuming more electricity than it can produce or buy from its neighbors." Source: http://www.iso−ne.com/nwsiss/pr/index.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

8. *April 28, Denver Post* — **Colorado highway closed by Hazmat spill.** A truck carrying hazardous materials tipped over on Loveland Pass in Frisco, CO, early Friday morning, April 28, shutting the highway down. The truck was hauling about six or seven different materials, including paint and phosphoric acid. Crews worked to keep the chemicals out of sources to Denver Water, the Snake River Water District and Dillon Reservoir. In addition to highway closure, access to the Arapahoe Basin ski area was cut off, for about five hours. Source: http://www.denverpost.com/news/ci_3762863

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

9. *April 28, SecurityFocus* — **Breach case could curtail web flaw finders.** Security researchers and legal experts have voiced concern over the prosecution of an information technology professional for computer intrusion after he allegedly breached a university's online application system while researching a flaw without the school's permission. On Thursday, April 20, the U.S. Attorney's Office in the Central District of California leveled a charge of computer intrusion against information technology professional Eric McCarty, alleging that he used a Web exploit to illegally access an online application system for prospective students of the University of Southern California (USC) last June. The security issue, which could have allowed an attacker to manipulate a database of some 275,000 USC student and applicant records, was reported to SecurityFocus that same month. The prosecution of the IT professional that found the flaw shows that security researchers have to be increasingly careful of the legal minefield they are entering when reporting vulnerabilities so as not to be accused of being a hacker, said Lee Tien of the Electronic Frontier Foundation. The case comes as reports of data breaches against corporations and universities are on the rise and could make security researchers less likely to bring flaws to the attention of Websites, experts told SecurityFocus. Source: http://www.channelregister.co.uk/2006/04/28/breach_suspect_p rosecuted/

10. *April 28, Associated Press* — **Pentagon hacker compromises personal data.** An intruder gained access to a Defense Department computer server and compromised confidential health

care insurance information for more than 14,000 people, the department said Friday, April 28. William Winkenwerder Jr., the assistant defense secretary for health affairs, said the affected individuals have been advised by letter that the compromise of personal information could put them at risk for identity theft. The Pentagon established a toll−free telephone number (1−800−600−9332) for affected people to call with questions. The computer server is for people insured under the Pentagon's TRICARE health care system. The type of information that was compromised was not disclosed, but Winkenwerder said it varied and investigators do not know the intent of the crime or if the compromised information will be misused. Routine monitoring of one of the health care insurance system's public servers detected unusual activity, and an investigation led to the discovery on Wednesday, April 5, that an intrusion had occurred and information was compromised. As a result, additional monitoring tools were installed to improve security of existing networks and data files, Winkenwerder said.
Source: http://www.startribune.com/587/story/400486.html

11. *April 27, DM News* — **Lycos adds anti−phishing toolbar.** Lycos launched a co−branded anti−phishing toolbar for consumers Wednesday, April 26, making it the latest search engine to alert consumers about phishing and identity theft while they are surfing online. Lycos and iS3 Inc. said they are launching a co−branded Lycos "securitybar" that consumers can download for free. The securitybar bases alerts on a list of known phishing sites from the Anti−Phishing Working Group as well as several other indicators. The toolbar also uses spyware protection, a "secure search" feature that erases users' search history and an ID Theft Prevention Package.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3662 4

12. *April 27, Websense Security Labs* — **Phishing Alert: Glacier Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of Glacier Bank. Users receive a spoofed e−mail message, which claims that they must confirm their account information due to recent changes in the bank servers. This e−mail message contains a link to a phishing Website and prompts the user to enter login information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =476

13. *April 27, United States Computer Emergency Readiness Team* — **Scripts in eBay postings may enable phishing attacks.** A vulnerability in the eBay Website may allow an attacker to steal personal information from eBay customers. eBay allows users to incorporate a type of code, also known as scripting, into the auction descriptions on its Website. An attacker can use this code to modify pages on eBay's Website or redirect a user to a malicious Web page. These may appear to be legitimate eBay Web pages that request personal information. Using these techniques, an attacker may be able to collect passwords, credit card numbers, or other personal information. US−CERT recommends that users ensure that the URL is accurate and check the Website certificate to ensure that the page is an authentic eBay Web page.
Source: http://www.us−cert.gov/cas/alerts/SA06−117Apr.html

14. *April 27, IDG News Service* — **Trojan horse freezes computer, requests ransom.** A new kind of malware circulating on the Internet freezes a computer and then asks for a ransom paid through Western Union Holdings Inc.'s money−transfer service. Graham Cluley of Sophos said the malware, which Sophos named Troj/Ransom−A, is one of only a few viruses so far that have asked for a ransom in exchange for releasing control of a computer. The new Trojan falls into a class of viruses described as "ransomware." The schemes had been seen in Russia, but

the first one appeared in English just last month. It's unclear how the Trojan is being spread, although Sophos is investigating, Cluley said. Once run, the Trojan freezes the computer, displaying a message saying files are being deleted every 30 minutes. It then gives instructions on how to send $10.99 via Western Union to free the computer. Hitting the Control, Alt, and Delete keys will not affect the bug, the virus writer warns. The virus writer even offers tech support, Cluley said. If the method of unlocking the computer doesn't work after the money is sent, the virus writer promises to research the problem and includes an e−mail address.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,110923,00.html

15. *April 27, Silicon.com* — **MasterCard security breach hits Morgan Stanley.** Morgan Stanley customers in the UK are the latest to have been hit by a major security breach that has resulted in thousands of MasterCard credit card details being stolen by scammers. At least 2,000 MasterCard holders have had their credit card details compromised. The Clydesdale Bank in the UK has admitted its customers were affected and now Morgan Stanley credit card holders have also been hit by the fraud. A Morgan Stanley spokesperson said: "The breach is something that has affected lots of issuers not just us. MasterCard informed Morgan Stanley [about the breach] and we are taking action to contact all cardholders affected, shut their accounts, and issue new cards." Some Visa cardholders have also contacted silicon.com to say they have had their cards canceled in the last week because of fraudulent activity on their account but Visa has so far been unable to confirm whether this is connected to the breach affecting MasterCard. Speculation is now growing that the UK incident could be linked to a massive security breach in the U.S. in April which resulted in hundreds of thousands of card details and PIN numbers being compromised by hackers.
Source: http://www.silicon.com/financialservices/0,3800010322,391584 48,00.htm

[Return to top]

Transportation and Border Security Sector

16. *April 28, Government Accountability Office* — **GAO−06−546: Changes to Deepwater Plan Appear Sound, and Program Management Has Improved, but Continued Monitoring Is Warranted (Report).** The Deepwater program was designed to produce aircraft and vessels that would function in the Coast Guard's traditional at−sea roles. After the terrorist attacks of September 11, 2001, however, the Coast Guard began taking on additional homeland security missions, and so it revised the Deepwater implementation plan to provide assets that could better meet these new responsibilities. While many acknowledge that the Coast Guard's aging assets need replacement or renovation, concerns exist about the approach the Coast Guard adopted in launching the Deepwater program. The subsequent changes in the program's asset mix and delivery schedules only increased these concerns. This report (1) compares the revised Deepwater implementation plans with the original plan in terms of the assets to be replaced or modified, and the time frames and costs for doing so; (2) assesses the degree to which the operational effectiveness model and other analytical methods used by the Coast Guard to develop the revised Deepwater asset mix are sound and appropriate for such a purpose; and (3) assesses the progress made in implementing the Government Accountability Office's (GAO) prior recommendations regarding program management. GAO is not making any new recommendations in this report.
Highlights: http://www.gao.gov/highlights/d06546high.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−546

17. *April 28, Department of Homeland Security* — **DHS introduces Maritime Infrastructure Recovery Plan.** The Department of Homeland Security announced Friday, April 28, the release of the Maritime Infrastructure Recovery Plan, one of eight plans supporting the National Strategy for Maritime Security. Key elements of the plan include guidelines for coordinated, national−level efforts to restore the flow of cargo and passenger vessels in response to a major disruption to the maritime transportation system. The plan also describes an exercise program that would be conducted periodically to assess the plan's effectiveness and the maritime community's ability to plan for, respond to, and recover from a national transportation security incident or incident of national significance. The Maritime Infrastructure Recovery Plan would be implemented by the Secretary of Homeland Security in the event of a significant national transportation security incident. The plan focuses on all forms of cargo, including those that are likely to hold perishable items in immediate need of unloading, or items that are key components in the production of consumer goods.
Additional information: http://www.dhs.gov/dhspublic/display?theme=67&content=4566
Source: http://www.dhs.gov/dhspublic/display?content=5583

18. *April 27, YNet News (Israel)* — **Warplanes meet Russian passenger jet that failed to identify itself after entering Israeli airspace.** Israeli Air Force fighter jets were mobilized on Thursday afternoon, April 27, to a Russian civilian plane, which was supposed to enter Israeli airspace −− but did not answer the control tower, in accordance with standard procedure. The fighter planes accompanied the Russian plane until it landed safely at an isolated runway at Ben Gurion Airport. It seems the problem was caused by some sort of technical problem in the communication network.
Source: http://www.ynetnews.com/articles/0,7340,L−3244700,00.html

19. *April 27, Pioneer Press (MN)* — **Arrest briefly shuts airport ticketing area.** The ticketing area at the Minneapolis−St. Paul, MN, International Airport Humphrey Terminal was shut down briefly Thursday morning, April 27, while airport police struggled with a man who became violent when officers tried to talk to him. Taye Birmachu was arrested for making terroristic threats and obstruction of justice.
Source: http://www.twincities.com/mld/twincities/14443507.htm

20. *April 27, Ananova (UK)* — **Serbian police fail to locate bomb used during drill.** As part of an exercise to test sniffer dogs at Surcin airport in Belgrade, the capital of Serbia and Montenegro, officers put explosives into luggage destined for Heathrow airport, as well as Paris, Milan, and Athens. The dogs found all the devices except one before Serbian police realized they had not marked the bags and could not find the final package or it's destination. Serbian authorities also failed to inform police in other countries about the incident, which took place on April 15.
Source: http://www.ananova.com/news/story/sm_1820248.html

21. *April 27, CNN* — **Security alert at Brussels airport.** Authorities evacuated and closed a busy terminal at Brussels' Zaventem International Airport after a man who was behaving suspiciously fled inside to evade a security check. Brussels Airport Inspections Service said there was a problem with a passenger, who passed security with something "suspicious" on his

back. The man was not found, police said.
Source: http://www.cnn.com/2006/WORLD/europe/04/27/belgium.alert/

22. *April 27, Government Accountability Office* — **GAO−06−588T: Gas Pipeline Safety: Preliminary Observations on the Implementation of the Integrity Management Program (Testimony).** About a dozen people are killed or injured in natural gas transmission pipeline incidents each year. In an effort to improve upon this safety record, the Pipeline Safety Improvement Act of 2002 requires that operators assess pipeline segments in about 20,000 miles of highly populated or frequented areas for safety risks, such as corrosion or welding defects. Half of these baseline assessments must be done by December 2007, and the remainder by December 2012. Operators must then repair or replace any defective pipelines, and reassess these pipeline segments for corrosion damage at least every seven years. The Pipeline and Hazardous Materials Safety Administration (PHMSA) administers this program, called gas integrity management, and inspects operators of interstate pipelines, while state pipeline safety agencies generally inspect operators of intrastate pipelines. This testimony is based on ongoing work for this Subcommittee and for other committees, as required by the 2002 act. It provides preliminary results on the safety effects of (1) PHMSA's gas integrity management program and (2) the requirement that operators reassess their pipelines at least every seven years. The Government Accountability Office (GAO) expects to issue two reports this fall that will address these and other topics.
Highlights: http://www.gao.gov/highlights/d06588thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−588T

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

23. *April 28, Illinois Ag Connection* — **University of Illinois Extension to upgrade system for diagnosing soybean rust.** University of Illinois Extension and the Illinois Department of Agriculture are collaborating on a new project that will improve the ability to rapidly diagnose Asian soybean rust and other plant diseases in Illinois. This joint project will significantly upgrade the Digital Distance Diagnostics Imaging System, which is already in use at Extension offices around the state of Illinois. This Internet−based tool enables plant pathologists at the University of Illinois to analyze leaf samples dropped off at any of one of the 95 Extension offices without leaving their lab.
Source: http://www.illinoisagconnection.com/story−state.cfm?Id=371&y r=2006

24. *April 28, North Dakota Ag Connection* — **Noxious weed infestations decline in North Dakota.** Leafy spurge edged out Canada thistle as North Dakota's worst noxious weed in 2005, but the reported acreage for both weeds was down slightly from 2004, according to a new report from the North Dakota Department of Agriculture. According to the report, overall

noxious weed−infested acreage fell from 3,375,479 reported acres in 2004 to 3,023,631 in 2005. The survey showed that infestations of all, but three, of the state's 12 noxious weeds declined between 2004 and 2005.
The 2005 North Dakota's Noxious Weeds Survey:
http://www.agdepartment.com/PDFFiles/NoxiousWeedListSurvey20 05.pdf
Source: http://www.northdakotaagconnection.com/story−state.cfm?Id=31 3&yr=2006

25. *April 27, SciDev.Net* — **Animal and plant diseases a growing threat in Africa.** A UK government program has warned that animal diseases will pose a growing threat in Africa unless the continent's health and veterinary services are significantly improved. The warning came Wednesday, April 26, in a study by the Foresight program. Of the world's 15 most important animal diseases, 12 occur in Africa. Such threats could grow in coming years as movements of people and animals increase and farming intensifies, predicts the report. It says tackling livestock diseases will be key to reducing rural poverty but that Africa lacks the resources and skilled personnel to achieve this.
Full report: http://www.foresight.gov.uk/Detection%20and%20Identification%20of%20Infectious%20Diseases/Index.htm
Source: http://www.scidev.net/gateways/index.cfm?fuseaction=readitem&rgwid=4&item=News&itemid=2807&language=1

[Return to top]

Food Sector

26. *April 28, U.S. Department of Agriculture* — **USDA releases Bovine Spongiform Encephalopathy prevalence estimate for U.S.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Friday, April 28, announced USDA's estimate of the prevalence of Bovine Spongiform Encephalopathy (BSE) in the United States. "Our enhanced BSE surveillance program has been an enormous undertaking, but well worth the effort," said Johanns. "We can now say, based on science, that the prevalence of BSE in the United States is extraordinarily low. The testing and analysis reinforce our confidence in the health of the U.S. cattle herd, while our interlocking safeguards, including the removal of specified risk materials and the feed ban, protect animal and human health."
An Estimate of the Prevalence of BSE in the U.S.:
http://www.aphis.usda.gov/newsroom/hot_issues/bse/content/printable_version/BSEprevalence−estimate4−26−06.pdf
Summary of Enhanced BSE Surveillance in the U.S.:
http://www.aphis.usda.gov/newsroom/hot_issues/bse/content/printable_version/SummaryEnhancedBSE−Surv4−26−06.pdf
Peer Review Agenda: http://www.aphis.usda.gov/about_aphis/printable_version/peer_review_plan_prevalence4−28−06.pdf
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/04/0143.xml

27. *April 28, Food Production Daily (UK)* — **Bovine Spongiform Encephalopathy on the rise in Poland.** Poland has confirmed a new case of Bovine Spongiform Encephalopathy (BSE) in one of its cows, as figures suggest the disease has crept forward in the country amid a rapid fall in

outbreaks elsewhere in the world. Poland's agriculture ministry said its routine sampling procedure had found a further case of mad cow disease in the country's Lodz province. Veterinary authorities said they had begun investigating how the cow became infected. Recent figures from the World Organization for Animal Health, show that cases of BSE in Poland have been increasing over the last few years. The figures also found BSE cases rising, albeit on a small scale, in the Czech Republic and Slovakia.
Source: http://www.foodproductiondaily.com/news/ng.asp?n=67381−bse−p oland−food−safety

28. *April 27, Nature Medicine* — **Sheep study calls for closer look at prion hypothesis.** The infectious agent behind diseases such as mad cow, scrapie and variant Creutzfeld−Jakob disease may not necessarily be rogue prion proteins, say British researchers. Although deformed prions are a characteristic of these diseases, they may not be the initial infectious agent, says lead researcher Martin Jeffrey of the UK'S Veterinary Laboratories Agency. The researchers are basing their theory on how these proteins are absorbed in the sheep gut. The scientists inoculated sheep intestines with brain extracts containing the abnormal form of the prion protein, the hallmark of the killer neurodegenerative disease. But when they later examined the infected sheep, the rogue protein had congregated at entirely different sites. The study also suggests that the mechanism of resistance against these diseases does not operate at the level of gut absorption, as some researchers had said.
Source: http://www.nature.com/news/2006/060424/full/nm0506−484a.html

29. *April 27, U.S. Food and Drug Administration* — **Pascal Company initiates worldwide recall anticavity treatment rinse.** Pascal Company, Inc., located in Bellevue, WA, is recalling all lots and all flavors of their products, NeutraGard 0.05% Neutral Sodium Fluoride Anticavity Treatment Rinse and NeutraGard Plus 0.2% Neutral Sodium Fluoride Anticavity Treatment Rinse, all flavors (Mint and Tropical Blast) packaged in clear 16 oz. plastic bottles because they may be contaminated with bacteria called Burkholderia cepacia and Pseudomonas aeruginosa. The problem was discovered during recent testing of samples stored for long−term studies conducted after the products were distributed. Only a small number of batches produced since 2001 showed the presence of these organisms, primarily in batches distributed prior to 2005.
Source: http://www.fda.gov/oc/po/firmrecalls/pascal04_06.html

30. *April 27, Food Production (Europe)* — **UK beef prices set to rise.** As the European Union's ban on UK beef exports comes to an end, continental demand for Britain's cheaper meat is expected to raise prices by up to a quarter. British beef exports across Europe have been restricted since the height of the Bovine Spongiform Encephalopathy scare, more than 10 years ago. And while cattle farmers were unable to secure export markets for their meat, supermarkets benefited from the reduced competition, driving prices down to artificially low levels. Now Duff Burrell of the National Beef Association thinks UK premium beef prices could rise to around $3.16 per kilo when the export ban is officially lifted by the European parliament on Tuesday, May 2, and ratified in Britain on Wednesday, May 3. And with a beef deficit across much of Europe, many suppliers have already placed orders with British abattoirs, which will impact supply and push up prices.
Source: http://www.foodproductiondaily.com/news/ng.asp?n=67321−meat− beef−bse

31. *April 26, Reuters* — **Estonia dismisses suspected case of mad cow disease.** Estonian authorities said on Wednesday, April 26, that tests for mad cow disease had proved negative in

the case of a dead 11−year−old animal earlier suspected of being the country's first case of Bovine Spongiform Encephalopathy.
Source: http://www.alertnet.org/thenews/newsdesk/L26272361.htm

[Return to top]

Water Sector

32. *April 27, Pantagraph (IL)* — **Rains bring end to drought.** The drought that began in March 2005 is officially over in Central Illinois, according to the National Weather Service. According the latest drought update, counties east of McLean County are classified as having no drought conditions. The counties of McLean, DeWitt, Woodford, Tazewell and Marshall and westward to Peoria are listed as abnormally dry. April showers have raised reservoir levels and soil moisture in Central Illinois and in most other regions of the state, said Illinois state climatologist Jim Angel. Just one town reservoir near Effingham remains low, he said. The only area of Illinois still considered in a moderate drought is a triangle of counties starting west of Peoria and extending to the Mississippi River. Portions of the northwest and southwest regions of the state remain dry. The 90−day forecast is neutral with regards to moisture and temperature predictions in the absence of strong weather patterns driving conditions one way or the other.
Source: http://www.pantagraph.com/articles/2006/04/27/news/doc44510d5203d92337435585.txt

[Return to top]

Public Health Sector

33. *April 28, BBC News* — **Cholera kills hundreds in Angola.** Cholera has killed 900 people in Angola in the past 10 weeks, says aid agency Medecins Sans Frontieres (MSF). Some 20,000 people are infected in several provinces and measures to contain the epidemic are inadequate, MSF says. Cholera is spread primarily by contact with contaminated water or food. Many Angolan homes lack running water and sewerage, after millions flocked to towns and cities amid 27 years of war. "Many factors have conspired to make this cholera outbreak one of the worst ever seen in Angola," says Richard Veerman of MSF. The week of April 24, MSF says it saw an average of 30 newly infected people and one death every hour. Tuesday, April 25, saw the highest daily toll so far, with 929 new cases and 25 deaths recorded by MSF. Over the past 10 years, Angola has suffered only minor outbreaks of cholera, mostly in isolated slum areas.
Source: http://news.bbc.co.uk/2/hi/africa/4953542.stm

34. *April 28, Associated Press* — **Tests: Indonesian man dies of bird flu.** Indonesia reported its 25th death from the H5N1 strain of bird flu on Friday, April 28, and China said an eight−year−old girl had contracted the disease. Citing local laboratory tests, Indonesia said its latest victim was a 30−year−old man who had come into contact with his neighbor's infected chickens. Samples have been sent to a World Health Organization−sanctioned laboratory in Hong Kong for confirmation, said Hariadi Wibisono, a director at the Health Ministry. If confirmed, the man's death will raise Indonesia's human toll from H5N1 to 25, Wibisono said. China reported its 18th case of the virus, 12 of which have resulted in death. The 8−year−old

girl from Suining, a city in the southwest province of Sichuan, showed symptoms of fever and pneumonia on Sunday, April 16, and was being treated at a local hospital, the Health Ministry said. Investigations show that poultry deaths were reported at her home before she got sick, the ministry said. Bird flu has killed at least 113 people since it began ravaging Asian poultry stocks in 2003.
Additional information included in above summary from:
http://www.cbsnews.com/stories/2006/04/23/health/printable15 34774.shtml
Source: http://www.nytimes.com/aponline/world/AP−Bird−Flu.html?_r=1&_oref=slogin

35. *April 28, Associated Press* — **CDC: Milder than normal flu season ending.** This year's flu season draws to a close as one of the mildest in recent years, partly because the vaccine was a good match for this winter's most common virus. Overall flu and pneumonia deaths were below those of a typical flu season, and health officials say fewer than two dozen children's deaths were reported. In about half of the states, reports of flu−like illness are sporadic or virtually nonexistent now, according to the U.S. Centers for Disease Control and Prevention. Flu was widespread in only five states −− Connecticut, Delaware, Indiana, New York, and Rhode Island −− the week of April 9−15. The long−lasting season started in December with a rush of cases in the Southwest. It then rotated to other regions, with widespread activity in some areas as late as April. This season, the number of deaths are lower than normal, possibly due to effective vaccines. Last year, health officials formulated the vaccine against three flu viruses −− Type A New Caledonia, Type A California, and Type B Shanghai. Of the patients who had Type A viruses, about 80 percent or more had viruses identical or similar to the A bugs in the vaccine.
Source: http://www.nytimes.com/aponline/us/AP−Flu−Season.html

36. *April 27, Reuters* — **Afghanistan finds five new cases of polio.** Afghanistan has found five cases of polio this year compared with one this time last year largely because people in some conservative areas are suspicious of immunization. Afghanistan is one of only four countries where the disease, which can paralyze a child within hours, is still endemic. The five new cases were all found in the southern province of Kandahar, three in the town of Spin Boldak on the Pakistani border. Health Ministry official Farooq Mojadidi said some families refused to get their children vaccinated against polio, believing it was part of a family planning campaign.
Source: http://news.yahoo.com/s/nm/20060427/hl_nm/polio_afghan_dc_1

37. *April 26, Associated Press* — **Law broadens quarantine powers.** While health officials propose broadening the federal government’s authority to declare quarantines, Iowa has given its health department similar power. Senate File 2322, signed Friday, April 28, by Governor Tom Vilsack, authorizes the Iowa Department of Public Health to enforce an area quarantine. The law also allows local health boards to implement quarantines, which would prohibit people from entering or leaving an area to prevent the spread of a sickness or hazardous materials. Health department spokesperson, Kevin Teale, said rules still must be drafted to define a quarantinable disease, the conditions of the quarantine and other specifics. Teale said his department asked lawmakers to consider expanding quarantine power as they discussed concerns of a possible pandemic flu and other rapidly spreading diseases. "As we reviewed current law, we did notice some things that we think needed some improvement...We hope it will help us more aggressively investigate possible illness and help get a handle on outbreaks earlier," he said. The law gives the department a legal avenue to force people to stay home. A limited quarantine was used in a measles outbreak centered in southeast Iowa in the spring of

2004.
Source: http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20060426/NEWS10/60426002/1001/NEWS

[Return to top]

Government Sector

38. *April 28, Department of Homeland Security* — **ICE arrests 125 alien fugitives and immigration violators in Midwest operation.** U.S. Immigration and Customs Enforcement (ICE) officers on Friday, April 28, arrested 106 illegal alien fugitives and 19 immigration status violators throughout the Midwest during a 10−day initiative. The operation, began April 10 and concluded April 19. The arrests of the fugitive aliens are the result of ICE's National Fugitive Operations Program (NFOP), which is part of ICE's ongoing effort to restore integrity to the nation's immigration system. The exclusive mission of the initiative is to reduce the number of fugitive aliens in the U.S., which is currently estimated at more than 597,000. These fugitives, or absconders, are foreign nationals who have been ordered removed by a federal immigration judge, but failed to comply with those orders and depart from the United States. The fugitives arrested during this operation include aliens from the following 28 countries: Cameroon, China, Congo, Costa Rica, Dominican Republic, Ecuador, El Salvador, Ethiopia, Ghana, Guatemala, Honduras, India, Indonesia, Ivory Coast, Jordan, Kenya, Kyrgyz Republic, Liberia, Lithuania, Mexico, Poland, S. Korea, Romania, Somalia, Tanzania, Thailand, Ukraine, and Yugoslavia.
Source: http://www.dhs.gov/dhspublic/display?content=5581

[Return to top]

Emergency Services Sector

39. *April 29, Arizona Republic* — **Massive disaster drill in Scottsdale involves about 3,000 people.** For the first time, civilian, medical and military forces gathered this week for an elaborate disaster drill in Scottsdale , AZ, that involved more than 3,000 people. The Coyote Crisis campaign, which ended Friday, April 28, responded to a fictional terrorist emergency characterized by explosions, poison gas and military evacuations. The massive four−day exercise involved the Arizona Air National Guard, Scottsdale Healthcare, General Dynamics, Scottsdale, Arizona State University and Luke Air Force Base in addition to Guard units from six other states. The participants typically hold separate disaster training exercises, planners said. The combined approach was designed to mimic real−world conditions.
Source: http://www.azcentral.com/news/articles/0429coyote0429.html

40. *April 28, Federal Computer Week* — **Los Angeles to deploy crime−analysis software.** Los Angeles County, CA, Sheriff's Department officials are planning to use sophisticated commercial crime−analysis software, Coplink, to help them piece together intelligence across millions of records and multiple databases in four systems. The systems include the Los Angeles Regional Crime Information System, which stores crime reports and arrest records for nearly half the county's cities, including Los Angeles; the Regional Allocation of Police Services, which houses computer−aided dispatch information; the Historical Automated Justice

Information and Jail Booking Systems; and the Crossroads Traffic System, which documents all county citations and traffic accidents.
Source: http://fcw.com/article94222−04−28−06−Web

41. *April 28, Telugu Portal (India)* — **Tsunami warning system to be tested May 16−17.** The first region−wide test of the Pacific Tsunami Warning System will be carried out May 16−17 to evaluate the response capabilities in countries in the region and improve coordination. There are 28 member countries in the Unesco/IOC International Coordinating Group of the Pacific Tsunami Warning and Mitigation System. The first stage will begin with a mock tsunami warning bulletin from the Pacific Tsunami Warning Center in Hawaii on May 16. The bulletin will be transmitted to designated contact points and national emergency authorities responsible for tsunami response in each country. In the second stage, which should be conducted on the same day or the following day, government officials will disseminate the message within the country to local emergency management and response authorities, simulating what would happen in a real situation.
Source: http://www.teluguportal.net/modules/news/article.php?storyid =3075

42. *April 27, Associated Press* — **Three−day drill to test Illinois' emergency preparedness.** Taking lessons they've learned from a previous statewide disaster drill, Illinois officials will test the state's ability to respond to a flu pandemic and a terrorist attack during a three−day exercise from May 2−4. The drill will focus on coordinating emergency responders and using state and local people and equipment to handle both a public health emergency and terrorist incident. "This is a really ambitious exercise and it was intended to stress our system so that we can find if there are weaknesses," said Patti Thompson, spokeswoman for the Illinois Emergency Management Agency. The event will test the state's capability to respond to two major disasters simultaneously as governments gear up against terrorist threats and the daunting prospect of widespread disease such as that posed by avian flu. U.S. Department of Homeland Security grants will pay for next week's $750,000 drill. It will involve 1,500 to 2,000 people from the state's Emergency Management Agency and departments of Transportation, Corrections, Public Health and Agriculture.
Source: http://www.belleville.com/mld/belleville/news/state/14445338 .htm

[Return to top]

Information Technology and Telecommunications Sector

43. *April 28, Reuters* — **Rhode Island embarks on wireless network.** America's smallest state is seeking to become its first to offer a wireless broadband network from border to border. Backers of Rhode Island's $20 million project say it would improve services and make the state a testing ground for new business technologies. It also comes at a time when Rhode Island's capital of Providence is stepping up efforts to lure business from Boston, about a 50−minute drive away, in neighboring Massachusetts, where office rents are among the nation's most expensive. The Rhode Island Wireless Innovation Networks should be fully in place by 2007, providing wireless connectivity throughout state, whose land mass of about 1,045 square miles is only slightly more than double the size of metropolitan Los Angeles.
Source: http://today.reuters.com/news/articlenews.aspx?type=domestic News&storyID=2006−04−28T204303Z_01_N28446626_RTRUKOC_0_US−RH

ODEISLAND.xml&pageNumber=0&imageid=&cap=&sz=13

44. *April 28, New York Times* — **New York county plans to offer free wireless Internet access.** Suffolk County, NY, is planning a wireless system to provide free access to the Internet to the 1.5 million residents who live throughout its 900 square miles. It would be one of the largest government−sponsored wireless networks in the nation. The system would allow anyone to use computers and PDA devices with wireless capabilities anywhere in the county, and would also be available to visitors, businesses, government agencies, institutions and groups. County officials hope to start installation next year. With Suffolk's extensive shoreline and the popularity of boating, officials are even exploring beaming signals over the water.
Source: http://www.nytimes.com/2006/04/28/nyregion/28suffolk.html?ei=5070&en=167376c6662ab1ec&ex=1146888000&adxnnl=1&emc=eta1&adxnnlx=1146261829−ZorCtOJabsOFcG6zrf+J+w

45. *April 27, Security Focus* — **Multiple Mozilla products memory corruption/code injection/access restriction bypass vulnerabilities.** Multiple Mozilla products are prone to multiple vulnerabilities. These issues include various memory corruption, code injection, and access restriction bypass vulnerabilities. Analysis: Garbage collection hazards have been found in the JavaScript engine where some routines used temporary variables that were not properly protected (rooted). Dynamically changing the style of an element from position: relative to position: static can cause Gecko to operate on freed memory. Calling the QueryInterface method of the built in Location and Navigator objects causes memory corruption that might be exploitable to run arbitrary code. XULDocument.persist() did not validate the attribute name, allowing an attacker to inject XML into localstore.rdf that would be read and acted upon at startup. An upgrade in the XML parser introduced a bug that could read beyond the end of the buffer, often causing a crash. The implementation of E4X introduced an internal "AnyName" object which was unintentionally exposed to Web content. Successful exploitation of these issues may permit an attacker to execute arbitrary code in the context of the affected application. This may facilitate a compromise of the affected computer.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/16476/info
Solution: Please see the referenced vendor advisories for details on obtaining and applying fixes: http://www.securityfocus.com/bid/16476/references
Source: http://www.securityfocus.com/bid/16476/discuss

46. *April 27, Security Tracker* — **Microsoft Internet Explorer bug in processing nested OBJECT tags lets remote users deny service.** A vulnerability was reported in Microsoft Internet Explorer. A remote user can cause denial−of−service conditions and may be able to cause arbitrary code to be executed on the target user's system. Analysis: The browser does not properly process certain combinations of nested OBJECT tags. A remote user can create specially crafted HTML that, when loaded by the target user, will trigger a NULL pointer dereference and cause the target user's browser crash. It may also be possible to execute arbitrary code, but code execution was not confirmed in the report. Affected version: 6. No solution was available at the time of this entry.
Source: http://securitytracker.com/alerts/2006/Apr/1016001.html

47. *April 27, Secunia* — **Microsoft Internet Explorer MHTML URI handler information disclosure vulnerability.** Microsoft Internet Explorer is prone to across domain information

disclosure vulnerability. Analysis: The vulnerability is caused due to an error in the handling of redirections for URLs with the "mhtml:" URI handler. This can be exploited to access documents served from another Website. Affected software: Microsoft Internet Explorer 6.x. Solution: Disable active scripting support.
Source: http://secunia.com/advisories/19738/

48. *April 27, Reuters* — **California agency approves broadband via power lines test.** The California Public Utilities Commission approved a plan on Thursday, April 27, allowing providers of high−speed Internet services to test using electricity lines to deliver online access throughout the state. Broadband over power lines, or BPL, could become a new competitor to Internet services delivered via telephone, cable and satellites and help reduce prices for consumers.
Source: http://today.reuters.com/news/articlenews.aspx?type=internetNews&storyid=2006−04−27T183248Z_01_N27428854_RTRUKOC_0_US−UTILITIES−BROADBAND−CALIFORNIA.xml&rpc=22

49. *April 26, CIO−Today* — **VoIP may be a future Denial of Service target.** Although there has yet to be a recognized instance of a VoIP−coordinated Denial of Service (DoS) attack, the Communications Research Network (CRN) says it is only a matter of time before the technique becomes mainstream. The CRN working group on Internet security has discovered a security loophole in VoIP applications that could give criminals operating on the Internet a better way of covering their tracks. According to CRN, VoIP tools could offer good cover traffic for DoS attacks because VoIP runs continuous media over IP packets. The ability to dial in and out of VoIP overlays allows for control of an application via a voice network, making tracing the source of an attack almost impossible. In addition, proprietary protocols inhibit the ability of ISPs to track DoS activity. CRN's Jon Crowcroft suggests that the loophole could be resolved if VoIP providers were to publish their routing specifications or switch over to open standards.
Source: http://www.cio−today.com/news/Is−VoIP−the−Next−Target−/story.xhtml?story_id=130004HC857W

50. *April 26, Federal Computer Week* — **Checklist outlines new cyberthreats.** The U.S. government and industry face many cyberthreats that, until now, have not received adequate attention, according to a new checklist outlining the threats. “We’re talking about vulnerabilities where we can calculate the effects, and the effects are considerable,” said Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit. The unit’s Cybersecurity Checklist looks at potential avenues for real−world cyberattacks and recommends ways to thwart them. The unit analyzed each of the 16 critical infrastructure sectors, Borg said. Many sectors say they follow international security standards but still have gaping security vulnerabilities, he said. Borg presented a draft version of the list at the GovSec conference in Washington, DC. The Department of Homeland Security has not yet approved the draft.
Source: http://www.fcw.com/article94201−04−26−06−Web

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 is aware of publicly available exploit code and materials explaining how to exploit a race condition vulnerability in Sendmail. Sendmail improperly handles asynchronous signals causing a race condition vulnerability. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user. For more information please review the following:

* TA06−081A − Sendmail Race Condition Vulnerability:
http://www.us−cert.gov/cas/techalerts/TA06−081A.html

* VU#834865 − Sendmail contains a race condition:
http://www.kb.cert.org/vuls/id/834865

* Sendmail MTA Security Vulnerability Advisory:
http://www.sendmail.com/company/advisory/

US−CERT recommends the following actions to mitigate the security risks:

* Upgrade to the latest version: Sendmail 8.13.6:
http://www.sendmail.org/releases/8.13.6.html

* Review the Sendmail MTA Security Vulnerability Advisory for steps to reduce the impact of this vulnerability:
http://www.sendmail.com/company/advisory/#mitigation

US−CERT is not aware of any working exploit code at this time.

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), 50497 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 4343 (unicall), 55620 (−−−), 135 (epmap), 139 (netbios−ssn), 80 (www), 1025 (win−rpc) 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

51. *April 28, WEWS−TV 5 (OH)* — **Police warn workers to watch for 'creepers'.** Police say employees −− especially those who work in large office buildings −− can be targets of identity thieves known as "creepers," reported WEWS−TV in Cleveland, OH. Police said building creepers walk through the front door like they belong there. "These folks blend right in. They dress the part, they act the part, they are very good at what they do," said Detective Ross Faranda. Police said creepers wander through office buildings unchallenged, looking for unlocked doors and unattended offices. Police said creepers canvass building hallways, searching for unattained purses, wallets, and valuables. Employee Sandy Stark said creepers got into her purse while she was at work. An unidentified woman then cashed a $765 check at a nearby bank just days later, easily posing as Stark. Thousands of dollars were fraudulently run up on Stark's credit cards. Farada says, "Everybody that runs a large office building should have a good video system and surveillance signs posted. That's number one." Fraud Detective Arvin Clar said, "Medical offices are a gold mine for criminal activity because of the amount of information available, especially doctor's offices and hospitals."
Source: http://www.kirotv.com/money/9069278/detail.html

52. *April 28, KVOA 4 (AZ)* — **Arson detectives investigate five suspicious fires in Arizona.** The Pima County, AZ, Sheriff's department is investigating five small, suspicious fires. Rural Metro Fire Department responded to three fires at the Holiday Inn on Palo Verde in Tucson. One fire was discovered in a bathroom on the first floor, another on the third floor, and the last behind the building. Another call came in from the 3400 block of East Pennslyvania where firefighters discovered two fires in two large dumpsters. Arson detectives are investigating. Guests at the Holiday Inn Palo Verde were quickly and safely evacuated Wednesday night, April 26. A guest first alerted hotel personnel. Arson Detective Jeff Whitbeck says he believes this is the work of arsonists, possibly juveniles.
Source: http://kvoa.com/Global/story.asp?S=4829823&nav=HMO6HMaY

53. *April 28, Associated Press* — **Man guilty of threat to bomb federal building in Milwaukee.** A man who authorities say idolized Oklahoma City bomber Timothy McVeigh was found guilty Thursday, April 27, of threatening to blow up a federal building in downtown Milwaukee, WI. A jury found Steven Parr, 41, guilty on the charge of threatening to blow up the Reuss Federal Plaza. Parr, of Janesville, could face up to life in prison. Parr had studied bomb−making books and previously built small explosive devices, prosecutors said. Authorities said Parr was days away from being released from state prison in September 2004 after serving time on drug charges when he told a cellmate about his plan to use a truck bomb to blow up the 14−story building. The cellmate alerted authorities.
Source: http://www.thestate.com/mld/thestate/news/nation/14447234.ht m

[Return to top]

General Sector

Nothing to report.
[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