Department of Homeland Security Daily Open Source Infrastructure Report for 20 January 2006

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

Daily Highlights

- The Associated Press reports Three Mile Island has investigated five incidents of inattentive −− an industry term that can mean sleeping −− employees in the past two years including two reports in December 2005. (See item 4)
- The Associated Press reports a Norfolk Southern train carrying sodium cyanide crashed in northern Alabama and at least 500 people were evacuated. (See item 17)
- U.S. Department of Health and Human Services has announced an initiative to transform the U.S. Public Health Service Commissioned Corps, which will enable this critical emergency response resource to address public health challenges more quickly and efficiently. (See item 30)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *January 19, Anchorage Daily News (AK)* — **Web post urges jihadists to attack Alaska pipeline.** A recent posting on a Website purportedly affiliated with al Qaeda urges attacks against the trans−Alaska oil pipeline and Valdez tanker dock, calling on jihadists to either shower the pipe with bullets or hide and detonate explosives along its length. The unknown

author encourages small cells of four or five mujahedeen, or Muslim guerrillas, living in the United States or in Canada or Mexico to mount the attacks. The 10−page posting includes numerous links to Websites providing maps and other basic information about the pipeline. The Arabic posting was discovered and translated in late December by the SITE Institute, a nonprofit organization that tracks international terrorists. Spokespersons for the FBI and other law enforcement and security agencies said they were aware of the posting, but none would say whether it had prompted any extra security measures in Alaska. Curtis Thomas, a spokesperson for the Alyeska Pipeline Service Co., said his company also was aware of the posting, but that "we're not aware at this time of any imminent threat" to the system. Eric Gonzalez, the FBI's Alaska spokesperson, said "We're in communications with state, federal and local law enforcement and private entities that would be affected by this."
Source: http://www.adn.com/front/story/7371578p−7283808c.html

2. *January 19, Bloomberg* — **U.S. storms, wind cut power to 450,000 from Boston to Carolina.** Storms with winds of up to 60 miles an hour knocked out power to about 450,000 homes and businesses on the East Coast and were blamed for two deaths. Karen Johnson, a spokesperson for Public Service Enterprise Group Inc., said, "This was pretty typical storm damage but some of our towers snapped in two..." About 104,580 customers lost power in northern New Jersey Wednesday morning, January 18, and service resumed to all but 15,000 by 3 p.m. EST. Exelon Corp.'s Philadelphia−based utility lost power to 54,000 customers, with service restored to almost half by 10 a.m. EST Wednesday. Northeast Utilities said that 107,691 of its customers in Connecticut were without service. According to Michael Clendenin, a spokesperson for Consolidated Edison Inc., 8,672 customers in the four boroughs surrounding Manhattan experienced power failures. Jersey Central Power & Light said that 6,000 customers lost power. Pepco Holdings Inc. restored electric service to all but 3,000 customers of the 50,000 who lost service. Dominion Resources Inc. lost power to more than 50,000 customers in Virginia and North Carolina, and by Thursday, January 19, 556 customers were still without power. National Grid PLC, said 43,700 customers in Massachusetts and Rhode Island lost power.
Source: http://www.usatoday.com/weather/stormcenter/2006−01−18−north east−winds_x.htm

3. *January 18, Reuters* — **Nigeria militants say all oil producers at risk.** Militants behind attacks aimed at disrupting Nigeria's oil exports said they will target all producers in the country, in a message singling out U.S.−based Chevron. The Movement for the Emancipation of the Niger Delta, which has caused major disruption at Royal Dutch Shell and kidnapped four foreign oil workers, said it has also attacked installations run by France's Total and Italy's Agip, a unit of ENI. "We have decided not to limit our attacks to Shell oil as our ultimate aim is to prevent Nigeria from exporting oil," the militant group said in an e−mail statement. Chevron has no plans to shut down production, according to spokesperson Don Campbell. Oil prices climbed to their highest level in almost four months on Wednesday as the group's threats exacerbated the markets' concerns. The militant group said, "Pipelines, loading points, export tankers, tank farms, refined petroleum depots, landing strips and residences of employees of these companies can expect to be attacked." Witnesses to attacks last week describe military−style operations involving around 40 trained militants, intelligence officials said. The group used a 12.7 mm heavy sub−machine gun mounted on a motor launch to attack one platform, they said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01

/18/AR2006011801812_pf.html

4. *January 18, Associated Press* — **Three Mile Island investigates incidents of inattentive employees.** The company that operates the Three Mile Island nuclear power plant said it has investigated five incidents of inattentive employees in the past two years including two reports in December. AmerGen Energy Co. hired an outside company to investigate a report last month that involved a shift manager, as well as how common inattentiveness is at the plant. Plant employees are not allowed to be inattentive, an industry term that can mean sleeping. The reports also involved security guards not responding promptly to employees waiting to enter the plant and an employee in a lunch room. In each case, the employee in question was disciplined by AmerGen, company spokesperson Ralph DeSantis said. None of the incidents affected the safe operation of the plant, he said. Eric Epstein, chairman of Three Mile Island Alert, a watchdog group, blamed the incidents on understaffing at the plant.
Source: http://www.centredaily.com/mld/centredaily/news/local/136538 01.htm

5. *January 18, Associated Press* — **Bureau of Land Management opens oil shale experiment on Western lands.** The U.S. Bureau of Land Management on Tuesday, January 17, selected the first companies that may have the chance to exploit vast oil−shale reserves in Colorado and Utah for petroleum. The reserves contain a 100−year domestic supply of oil, although it's locked up in layers of hard rock and the technology for economically recovering it is still evolving. Tuesday's announcement amounted to tentative approval for experimental works, but more significantly it put major oil companies and a few small players in line for leasing larger federal tracts for commercial operations that could start as early as mid−2007.
Source: http://www.heraldextra.com/content/view/160147/

6. *January 18, South Florida Sun Sentinel* — **Florida Power & Light may exceed standards to ensure reduced damage to poles during hurricanes.** Florida Power & Light Co.'s (FPL) utility poles were up to −− and even exceeded −− industry standards before Hurricane Wilma last October, according to KEMA Inc., an international engineering company. But for hurricane−prone Florida, the firm said those standards may not be high enough. "It is worth considering the possibility of using criteria exceeding minimum code standards in an effort to reduce the extent of damage that can be expected during extreme wind conditions," said KEMA's report. Wilma caused extensive damage to the infrastructure of the utility: more than 11,000 distribution poles and nearly 100 transmission structures were affected. The report provided insight into which parts of FPL's infrastructure failed and what the utility needs to improve. Wood poles for the transmission lines met the required design codes at the time of installation, but FPL now is using an updated design. FPL will seek ways to improve its installation of crossbrace bolts on the transmission−line structures, which caused 30 tower failures. FPL substation outages, thought to be the prime cause for electrical failure after Wilma, were mostly due to transmission−line problems. KEMA's data only pertains to FPL−owned poles. The damaged−pole issue is complicated because many Florida utilities share poles.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpp%5E%5BflqsuroTTmj%7D38%7Dbfel%5Dv

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

7. *January 18, Air Force Link* — **Air Force to replace combat search and rescue helicopters.** Air Force combat search and rescue (CSAR) teams will use a new helicopter −− the now under development CSAR−X −− to help recover downed pilots around 2012. The new helicopter will replace 101 HH−60G Pave Hawk helicopters Air Force combat search and rescue teams now use. The Air Force expects to begin purchasing the new aircraft by fiscal 2009, with delivery by fiscal 2011. They will be operational in fiscal 2012. The cost of the new system is not yet determined because it will be based on the final source selection, said Lt. Col. Dave Morgan, combat search and rescue program element monitor for Air Force acquisition. The Air Force must enhance the Pave Hawk fleet's size and availability for use by combatant commanders, said Lt. Col. Michael T. Healy, Air Force deputy division chief for mobility, combat search and rescue and special operations requirements. The Air Force is considering several replacements for the HH−60. They are all based on existing helicopters which need modification to meet Air Force needs. The acquisition strategy takes an existing aircraft and adds the capabilities needed for the CSAR mission.
   Source: http://www.af.mil/news/story.asp?id=123014552

8. *January 18, Defense News* — **China focuses on lasers, technology.** The Chinese government has announced a 15−year plan to improve China’s ability to develop and produce innovative technology. The plan may boost the Chinese military as well as strengthen China’s clout in the world’s technology industry, two technology experts said Wednesday, January 18. China’s plan calls for “greatly strengthening independent innovation” in technology fields related to energy, space, the military, environment and urban development, said William Archey, president of the American Electronics Association. And as China develops better technology, its military will be a major beneficiary, said Adam Segal, author of “Digital Dragon: High−Technology Enterprises in China.” One area where China is already focusing substantial research is lasers, Archey said. It is unclear, for now, whether the lasers are being developed for military or commercial purposes, he said. The new push to develop more innovative technology comes atop Chinese efforts to modernize its military by buying more advanced technology from Russia and other countries, Segal said. Despite a wide range of export controls imposed by the U.S. to keep sensitive military and “dual use” technology from being sold to China, it will be difficult for the U.S. to stop other countries from selling such technology to China, Segal said.
   Source: http://www.defensenews.com/story.php?F=1475734&C=asiapac

[Return to top]

Banking and Finance Sector

9. *January 19, Reuters* — **Fingerprint checks coming to banks.** According to the consulting firm Accenture, within five years, branches at major banks across the globe are likely to

embrace cutting−edge technology such as radio frequency identification and biometric scanning. Simon Jenkins, retail banking partner for Accenture in the United Kingdom, said "Banks are trying to differentiate themselves and branches are still fundamental to this, so they are trialing lots of this new technology." Radio frequency identification, or RFID, is a technology being developed that should migrate to banks. Customers would be automatically identified by the RFID−encrypted card in their wallet as they pass through the door. By the time the customer reaches the counter all his or her details would be displayed on the teller's screen. "The bank wants to be able to identify the customer the minute they walk in and understand why they are there," said Mike Redding, head of development for Accenture Technology Labs. Demand for anti−fraud measures should see advances in biometrics −− fingerprint or eye, facial, palm, voice, vein or even ear shape recognition software −− operated by bank staff or included in an automated teller machine.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/19/AR2006011901074.html

10. *January 18, Reuters* — **India sets up IT and call center database to fight fraud.** India's booming information technology and call center industry launched a database for its workforce on Wednesday, January 18, that it hopes will boost data security after reports of theft surfaced last year. The sector directly employs a million people, and indirectly about three times that number in jobs ranging widely from transport and security to catering and housekeeping, and vowed last year to better monitor its employees and raise privacy standards. The database containing personal and work−related information would enable employers to verify a staff member's credentials while police would be able to track the background of workers. India's call centers were hit in April 2005 by a $400,000 online credit card fraud after workers enticed bank customers to part with personal details. A month later a British newspaper alleged that a call center worker illegally sold secret data of British bank customers to an undercover reporter. According to the National Association of Software and Service Companies, the database is a world first for the IT industry. "Information security is an integral part of the information infrastructure for enhancing India's e−business environment," said T.D. Maran, federal minister for communications and information technology.
Database: http://www.nationalskillsregistry.in.
Source: http://news.yahoo.com/s/nm/20060119/tc_nm/india_database_dc_2

11. *January 18, Culpeper Star Exponent (VA)* — **Bank customers urged to avoid scam.** Second Bank & Trust is urging its customers to ignore an e−mail scam phishing for personal financial information. The e−mails, which look as though are sent by the bank, claim Second Bank & Trust is launching a new security system and needs to confirm the account holder’s authenticity or that its bill pay service is being renewed and will cancel if information is not provided. marketing director Tuck Pulliam said, "Obviously we do not send e−mails to anybody asking for that type of information...We have been made aware of these phishing attempts and we have alerted the proper law enforcement agencies.” Pulliam said customers and non−customers in Culpeper, VA, and surrounding areas were targeted.
Source: http://www.starexponent.com/servlet/Satellite?pagename=CSE/MGArticle/CSE_MGArticle&c=MGArticle&cid=1128769383327

12. *January 18, Vnunet.com* — **U.S. Marine scam e−mail hits inboxes.** Security companies are warning of a new e−mail scam that is posing as a letter from a U.S. Marine serving in Iraq. The

e−mail is a variant of the standard 419 scam, where huge riches are promised if the recipient hands over their bank account details and pays an ever increasing number of commissions and bribes. The message reads: "My name is Sgt Richard Murphy, I am in the Military Engineering Unit here Baghdad, Iraq. We have about $15 million U.S. dollars that we want to move out of the country. My colleagues and I need a good partner, someone we can trust. This is a risk free and legal business (oil money)." Such scams tend to follow the headlines and past examples have included e−mails purporting to be from the Thatchers in South Africa as well as the relatives of leaders from the Congo, Yugoslavia, and Afghanistan.
Source: http://www.infomaticsonline.co.uk/vnunet/news/2148813/marine−scam−email−hits−inboxes

13. *January 18, CNET News* — **More brands targeted as phishing attacks soar.** Phishing attacks reached a new high at the end of 2005 after growing steadily all year, according to the Anti−Phishing Working Group in a new study. The number of unique e−mail−based fraud attacks detected in November 2005 was 16,882, almost double the 8,975 attacks launched in November 2004. The number of brands targeted increased by nearly 50 percent over the course of 2005, from 64 to 93 percent in November. Despite these statistics, businesses should not worry about the effect on consumer confidence, according to Internet security company Websense. Mark Murtagh of Websense said "Although phishing is increasingly in the news, online banking is increasing in popularity." Top brands continue to be hijacked; most phishing sites spoof global e−commerce and banking institutions. "eBay is often spoofed...Google is increasingly being targeted because of its expansion into different business application models. The big banking names are used too −− HSBC, Citigroup, Lloyds −− all the major brands," he said. Attacks are becoming increasingly sophisticated, with a quarter of all phishing Websites hosting keylogging malicious software. Users can become infected just by visiting the sites, Murtagh warned. "Now with most phishing sites they just have to visit one to become infected."
Report: http://antiphishing.org/reports/apwg_report_Nov2005_FINAL.pdf
Source: http://news.com.com/More+brands+targeted+as+phishing+attacks+soar/2100−7349_3−6028338.html?part=rss&tag=6028338&subj=news

[Return to top]

Transportation and Border Security Sector

14. *January 19, Associated Press* — **California panel report criticizes 'push' configuration for passenger trains.** More than 600 Californians have been killed or injured in collisions with trains at public grade crossings since 2001, one of the worst records in the United States, according to a report by a state panel released Wednesday, January 18. "California continues to rank as one of the six worst states in the country regarding the number of accidents and fatalities at public grade crossings," the report by the state Assembly Special Committee on Rail Safety stated. The report also recommends passenger railroads stop using locomotives to push trains from behind and adopt other safety measures to reduce the carnage. "There are allegations that pushed trains are more likely to derail because the lighter passenger cabs in the front can be pushed off the tracks more easily," the state report said. Thirteen people have been killed since 1992 in collisions involving Amtrak trains in push mode while no passengers have died in collisions involving trains in pull mode, the report said. "We respectfully disagree with the committee's conclusion on push−pull," said Denise Tyrrell of Metrolink, the Southern

California regional passenger rail system. "As it stands, commuter rail cars are 20 times safer than an automobile," she said.
Rail safety report: http://democrats.assembly.ca.gov/members/a43/mainpage.htm
Source: http://www.contracostatimes.com/mld/cctimes/news/state/13656 652.htm

15. *January 19, Associated Press* — **Report: Tunnel could be built to extend Los Angeles subway to beach.** A subway tunnel that would run beneath a major thoroughfare and connect downtown Los Angeles with the beach and the city's crowded west side can be safely built despite high levels of methane gas, according to a report by the American Public Transportation Association's peer review panel. The panel's study showed that pressure−balanced tunneling machines could bore below Wilshire Boulevard without encountering any problems. Strong ventilation, regular testing of gas pressure and precast tunnel liners also would ensure the project's safety, according to the report, which was reviewed Wednesday, January 18, by the City Council. “This is an issue that will be coming back before us many times," said Councilwoman Wendy Greul. "We know this is critical to the gridlock that we're seeing ...” Transit officials estimate it would cost about $4 billion to build the subway tunnels that would extend the Red Line, which currently runs 17 miles from downtown to the San Fernando Valley.
Source: http://www.signonsandiego.com/news/state/20060118−2313−ca−la subwaytunnel.html

16. *January 19, Associated Press* — **New Yorkers to get subway cell service.** Several major wireless carriers submitted bids Wednesday, January 18, to wire 277 New York subway stations for cell phone use, including one proposal that involves four of the nation's biggest carriers forming an alliance. The bids mark a significant step in a long−running effort to make cell phone service available to the millions of New Yorkers who lose mobile phone communications when using the subways. The 10−year contract calls for the winning bidder to wire only the platforms and not moving trains. But the companies were required to discuss how they would expand the network to the tunnels. Whoever wins the contract would have to let other carriers use the network, Metropolitan Transportation Authority spokesperson Tom Kelly said. It is not clear if wiring the subways will pay off. Industry experts said it made sense for the companies to form a partnership to allay the costs. Jonathan Spira, chief analyst at Basex, an IT research firm in New York City, said the real "pot of gold at the end of the rainbow" for the companies was in the wiring of the trains −− not in merely making it possible for commuters to talk while waiting on the platforms.
Source: http://www.cnn.com/2006/TECH/ptech/01/19/wired.subway.ap/

17. *January 19, Associated Press* — **Alabama train mishap sparks fire, evacuation.** The wreckage of a fiery crash involving a train carrying sodium cyanide continued to burn Thursday, January 19, but no hazardous chemicals were detected in the air, officials said. The fire mostly involved paper and automobile parts, said Jerome Hand, a spokesperson for the state environmental management agency. Hand said air tests showed no danger from chemicals. The train car carrying the chemical was not apparently breached, said Susan Terpay, spokesperson for Norfolk Southern, which operates both trains. About 500 people had been evacuated after the crash Wednesday evening, January 18, in northern Alabama, and some were allowed to return Thursday. Three crewmembers were treated at a hospital. The train carrying the chemical had rammed the back of another train, carrying automobiles, that had pulled onto side rails to let it through, but not all of the first train's 81 cars cleared the main tracks, Terpay said. The fire

created a plume of black smoke that could be seen 40 miles away in Birmingham, and about 500 homes within a mile of the blaze were initially evacuated.
Source: http://www.newsday.com/news/nationworld/nation/sns−ap−train−collision,0,1530865.story?coll=ny−leadnationalnews−headlines

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

18. *January 19, Associated Press* — **Deer are killed over chronic wasting disease concerns.** Government sharpshooters killed 76 deer at a central Wisconsin game preserve where a number of animals have been found to have chronic wasting disease (CWD). The U.S. Department of Agriculture's wildlife services unit killed the deer on Tuesday, January 17, in an enclosure at the Portage County preserve. Donna Gilson of the state Department of Agriculture, Trade and Consumer Protection said carcasses of three other deer were found, and all 79 deer will be tested for CWD. Sharpshooters still had to kill about 40 bucks in a separate enclosure. That enclosure is where a hole was found in the fence last week, causing concern that some of the deer might have been able to leave. Over the weekend, personnel from the state Department of Natural Resources killed two does and two fawns in the area outside the fence.
CWD information: http://www.cwd−info.org/
Source: http://www.greenbaypressgazette.com/apps/pbcs.dll/article?AID=/20060119/GPG0204/601190482/1233/GPGsports

19. *January 18, United Press International* — **Warm U.S. weather poses crop risk.** For the third consecutive week above−normal temperatures prevailed across the U.S. last week, exposing some crops to risks. Throughout the northern Great Plains and most of the Corn Belt and Ohio Valley, average temperatures exceeded normal causing further depletion of protective snow cover in these regions, the U.S. Agriculture Department said Wednesday, January 18. Dry conditions persisted in the Great Plains and Southwest, further depleting soil moisture. However, moderate precipitation in the upper Delta and eastern Corn Belt helped winter wheat in those areas. Moderate to heavy precipitation in the Pacific Northwest improved soil moisture in the inland crop producing areas while increasing snow pack in the higher elevations. Warm weather in California has deterred dormancy in fruit trees and caused blooming in some orchards, while lingering wet conditions in some areas caused worsened small grain condition and delayed vegetable harvest. In Texas, winter wheat was rated mostly poor to very poor due to extremely warm temperatures and dry, windy conditions. Warm weather in Georgia increased insect activity and the spread of disease in pastures but improved small grain conditions.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20060118−05004 9−2939r

20.

January 18, Pantagraph (IL) — **Animal identification system to be tested.** The Illinois' counties of Livingston, Stephenson, and Bond have been selected as participants in an animal identification pilot project for county fairs. The project will operate as a partnership between Illinois Farm Bureau (IFB) and the University of Illinois Extension. The goal centers on attaching radio frequency identification tags to animals before the fair, scanning tags at the fair, and checking tag retention. "Like Illinois livestock farms, county fairs are going to have to have premise numbers and be able to trace movement of animals that show there," said Jim Fraley, IFB livestock specialist. Information from the reader will be downloaded to a laptop computer. "The data won't be reported anywhere. We want to find any pitfalls or unanticipated problems. Will there be problems installing the tags? Will the tags get ripped off before the fair? Will the reader easily record the tag information," Fraley asked. Dave Seibert, U of I Extension area livestock specialist, said the project should further show which types of tags best fit separate species. Fraley and Seibert hope to use the pilot project findings to help fairs across the state prepare for national mandatory animal identification requirements in 2008.
Source: http://www.pantagraph.com/articles/2006/01/18/business/10402 7.txt

[Return to top]

Food Sector

21. *January 19, San Antonio Express−News (TX)* — **Meat distributor admits trying to trick Mexico.** On Wednesday, January 18, the owner of a San Antonio, TX, wholesale distributor of meat and poultry products pleaded guilty to charges his company tried to bypass Mexico's ban in 2002 on chicken originating in Texas by misrepresenting that about 35,000 pounds of frozen chicken leg quarters came from another state that was not part of the ban. The ban was implemented in response to the appearance of exotic Newcastle disease in some chickens raised in Texas. Specifically, the company tried to export 858 cases, each case weighing about 40 pounds, of frozen chicken leg quarters into Mexico, court records show. The 858 cases in question were from a Texas producer but the original labels were removed and replaced with labels stamped with a federal mark of inspection for an Alabama producer, according to court records. On June 28, 2002, agents with the U.S. Department of Agriculture inspected the cases at the ADT warehouse and found the chicken had been purchased from a producer in Dallas, TX, agent Eduardo Vendrell said in an affidavit.
Source: http://www.mysanantonio.com/news/metro/stories/MYSA011906.05B.chicken_run.17827394.html

22. *January 18, Arizona Republic* — **Second unlicensed slaughterhouse closed.** Just days after a Tolleson, AZ, area meat merchant pleaded guilty to running an unlicensed slaughterhouse, his brother also was ordered to close his business after slaughtering animals and selling meat to the public. This is the second time in four months that an illegal slaughterhouse in the Southwest Valley has been forced to close, state and Maricopa County authorities said Wednesday, January 18. Rafael Serrato, who operated a meat business near Tolleson, is accused of selling meat without a permit and illegally dumping the remains of cattle, goats, and pigs. An Arizona Department of Agriculture inspector observed more than a dozen pigs and several goats killed by rifle, while "at least 10 men worked at slaughtering the animals." Numerous customers also were seen placing orders and picking up meat. County authorities also found that a 240−pound pig purchased at the business by an undercover inspector tested positive for chronic viral

pneumonia and bore scars from bacterial−type pneumonia. Serrato's brother, Jose Merced Serrato−Maciel, last week pleaded guilty to selling insect−laden and disease−causing meat products to the public. His company, which had no formal name was forced closed September 20, 2005.
Source: http://www.azcentral.com/news/articles/0118slaughter18−ON.ht ml

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

23. *January 19, World Health Organization* — **WHO calls for an immediate halt to provision of single−drug artemisinin malaria pills.** The World Health Organization (WHO) Thursday, January 19, requested pharmaceutical companies to end the marketing and sale of "single−drug" artemisinin malaria medicines, in order to prevent malaria parasites from developing resistance to this drug. The use of single−drug artemisinin treatment −− or monotherapy −− hastens development of resistance by weakening but not killing the parasite. When used correctly in combination with other anti−malarial drugs in Artemisinin Combination Therapies (ACTs), artemisinin is nearly 95 percent effective in curing malaria and the parasite is highly unlikely to become drug resistant. ACTs are currently the most effective medicine available to treat malaria. "It is critical that artemisinins be used correctly," said Lee Jong−wook, WHO's Director−General. "We request pharmaceutical companies to immediately stop marketing single−drug artemisinin tablets and instead market artemisinin combination therapies only." According to the new WHO malaria treatment guidelines, uncomplicated falciparum malaria must be treated with ACTs and not by artemisinin alone or any other monotherapy. "So far, no treatment failures due to artemisinin drug resistance have been documented, but we are watching the situation very attentively," said Arata Kochi, the newly appointed director of WHO's malaria department.
Source: http://www.who.int/mediacentre/news/notes/2006/np02/en/index .html

24. *January 19, Daily Times (NM)* — **Woman dies of hantavirus.** An Arizona woman, who lived on the Navajo Nation in New Mexico, died of Hantavirus Pulmonary Syndrome (HPS), which is caused by the hantavirus, an Indian Health Services official said. The Native American woman died in December, but the cause of her death wasn't confirmed until this month, said Jenny Notah, associate director for the office of program planning and evaluation for the Navajo Area Indian Health Service. "The only information is that the case did occur in northern Arizona and she was a Native American female. We don't provide the name and location of the victim," said Notah. This was the first HPS−related death on the reservation since April 2005, Notah said.
HPS information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://www.daily−times.com/apps/pbcs.dll/article?AID=/200601 19/NEWS01/601190301/1001

25. *January 19, Agence France−Presse* — **Bangladesh to launch world's biggest measles vaccination drive.** More than 33 million children in Bangladesh will be vaccinated in February in the world's largest measles vaccination campaign. Measles kills around 20,000 children each year in Bangladesh. "We will start the nationwide anti−measles campaign from February during which a total of 33.5 million children will be vaccinated against measles," government health ministry spokesperson Golam Kibria said. "The plan is to wipe out measles once for all from Bangladesh soil," Kibria said. "Bangladesh has one of the highest child mortality rates from measles. The campaign will be the world's biggest−ever measles vaccination program," said United Nations Children's Fund spokesperson Kirsty McIvor. Vaccination centers would be set up in over 260,000 schools, hospitals, and other public buildings, Kibria added. Most developed countries routinely vaccinate children against measles but the virus still kills an estimated 500,000 people globally each year.
Measles information: http://www.cdc.gov/ncidod/diseases/submenus/sub_measles.htm
Source: http://news.yahoo.com/s/afp/20060119/hl_afp/bangladeshhealthchildrenunicef_060119142657;_ylt=AimVeyNBILESLyYw9ydB5pWJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

26. *January 19, Agence France−Presse* — **Concern over China's surveillance methods after sixth bird flu death.** China's bird flu surveillance methods were again under the spotlight after it was revealed the latest human H5N1 fatality occurred in an area where no outbreak among poultry had been reported. China announced on Wednesday, January 18, that a 35−year−old woman from Jianyang city, in the southwestern province of Sichuan, had become the nation's ninth confirmed human case of bird flu and its sixth fatality from the disease. No outbreak of the disease among poultry had been reported in Jianyang city, with the closest H5N1 outbreak recorded in Sichuan's Dazhu county 150 miles away. "We have asked the Ministry of Health to clarify if the death was linked to the Sichuan outbreak (among birds) reported earlier," said Roy Wadia, the Beijing spokesperson for the World Health Organization. Wadia expressed concern that seven of the nine human cases in China had occurred in areas where no poultry outbreaks had been reported. "Human cases should not be the sentinels for animal outbreaks," Wadia said. "Ideally we should be able to find the animal cases first and allow health authorities to scour the region to find human cases."
Source: http://news.yahoo.com/s/afp/20060119/hl_afp/healthfluchinawho_060119112125;_ylt=AgG9jg4O9WqRqfByPCD4rpeJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

27. *January 19, Xinhua (China)* — **Hong Kong finds H5N1 positive wild bird carcass.** A dead wild bird in Hong Kong has been confirmed to be positive for the H5N1 strain of bird flu, local authorities announced on Thursday, January 19. "In Hong Kong, it's the first time we have found the virus on the species," said an official from the Agriculture, Fisheries and Conservation Department of the Hong Kong Special Administrative Region (HKSAR). However, "there's no cause of alarm," said the official, for patrol conducted in the area had found no avian influenza on poultry farms. Neither did a further survey of Hong Kong's other poultry farms find bird flu, the official told a news conference. The body of the wild bird, a magpie robin, was collected on January 10 in Tai Po. Previous to this case, Hong Kong has kept a zero−outbreak record and the authorities have launched aggressive campaign to prevent the disease from entering the territory.

Source: http://news.xinhuanet.com/english/2006−01/19/content_4074761 .htm

28. *January 19, Financial Times (United Kingdom)* — **International community pledges $1.9 billion for bird flu self−defense.** The international community Wednesday, January 18, promised $1.9 billion to fight avian flu in the worst−affected countries, with the largest commitments coming from the U.S. with $334 million and the European Union pledging $260 million. The funding, promised at an international conference in Beijing, China, was well in excess of an initial target set by the World Bank to raise at least $1.2 billion. The amount raised is evidence of the heightened worries surrounding the potential economic fallout of even a regional epidemic of H5N1 −− the strain which has killed at least 79 people. Governments and global health organizations have been trying to come up with a financing plan since November. The world's top public health authorities stressed the critical next step would be to devise a strategy to allocate the money to desperate governments while ensuring the funds could be accounted for. Lee Jong−Wook, director−general of the World Health Organization, told the Financial Times he expected the task of distributing the funds to countries would be "very complicated." There are widespread concerns that an unmanageable outbreak or virus mutation in a single country may quickly spread beyond borders.
Source: http://news.ft.com/cms/s/be9f2290−888f−11da−a25e−0000779e234 0.html

29. *January 19, Agence France−Presse* — **Crippling disease sweeps Indian Ocean island.** Doctors on the Indian Ocean island of Reunion are battling an epidemic of a crippling mosquito−borne disease that has no known cure, French Health Minister Xavier Bertrand said. About 7,200 cases of chikungunya had been recorded, including 1,600 cases last week alone, the minister told the French upper house. Chikungunya is Swahili for "that which bends up" and refers to the stooped posture of those afflicted by the non−fatal disease for which there is no known vaccine or cure. Authorities on the volcanic island east of Madagascar, a French overseas department with a population of 760,000, have earmarked $720,000 to fight the outbreak, including special mosquito−eradication brigades.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://www.breitbart.com/news/2006/01/19/060119182521.mgm4qa hf.html

30. *January 18, U.S. Department of Health and Human Services* — **New initiative announced to transform the U.S. Public Health Service Commissioned Corps.** U.S. Department of Health and Human Services (HHS) Secretary Mike Leavitt Wednesday, January 18, announced an initiative to transform the U.S. Public Health Service (USPHS) Commissioned Corps, which will enable this critical emergency response resource to address public health challenges more quickly and efficiently. The Commissioned Corps will increase its ranks, streamline its assignment and deployment process, and increase its ability to recruit. In remarks before officers, Secretary Leavitt outlined his vision of the USPHS as an essential national resource to meet HHS' critical mission requirements; ready to respond rapidly to urgent public health challenges and emergencies; available to address needs in isolated, hazardous or other difficult−to−fill positions; and sought at the federal and state levels to help meet essential public health leadership and service roles. Over the next two months, strategies will be developed to increase the size of the corps and improve its ability to respond quickly to urgent public health needs. The Commissioned Corps seeks to: increase the number of officers by 10 percent, to a total of 6,600 members; improve response operations and team−oriented deployment process; and change the recruitment process so that it includes stronger personal

incentive programs and a better approach for assigning officers.
USPHS Website: http://www.usphs.gov/
Source: http://www.hhs.gov/news/press/2006pres/20060118.html

31. *January 17, Angola Press Agency* — **Unidentified disease kills two in Angola.** A strange disease broke out and has killed two people since December in Nharea, Angola. The information was released on Tuesday, January 17, by Documentation and Information Center that said 10 people caught the disease since it broke out in the region, two of whom died. According to the source, fever and blisters followed by the deterioration of the skin are the symptoms. Meanwhile, the head of Department of Public Health and Control of Endemics, José Augusto Gonçalves, said his sector has not yet been notified about the disease. However, he said a technical team will be sent soon to Nharea to probe into the origin of the disease.
Source: http://allafrica.com/stories/200601170882.html

[Return to top]

Government Sector

32. *January 19, Associated Press* — **Small fire at Pentagon causes damage.** A fire broke out in a third−floor kitchen stove Thursday, January 19, and spread to ductwork that passed through the fourth and fifth floors to the roof, authorities said. The blaze was quelled, said Arlington County (VA) Fire Department spokesperson Tom Polera, but the process of cleaning up and checking the damaged area for hot spots was continuing, complicated by asbestos surrounding the ductwork. Areas of the building near the ductwork were temporarily closed to keep personnel from possible contact with asbestos, Polera said. No one was injured in the fire. Damage was estimated at $200,000.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=46058

33. *January 19, The White House* — **Personnel announcement: President Bush nominates new Coast Guard commandant.** President George W. Bush on Thursday, January 19, announced his intention to nominate Vice Admiral Thad W. Allen to be Commandant of the United States Coast Guard. Vice Admiral Allen currently serves as Chief of Staff for the Coast Guard. He also served as the Principal Federal Official overseeing Hurricane Katrina response and recovery efforts in the Gulf Coast region. Vice Admiral Allen previously served as Commander of the Coast Guard Atlantic Area, Fifth United States Coast Guard District, and the United States Maritime Defense Zone, Atlantic Fleet. In addition, he led the Atlantic forces in the Coast Guard's response to the terrorist attacks on September 11, 2001. Prior to that position, Vice Admiral Allen commanded the Seventh Coast Guard District and was the Director of Resources for the Coast Guard. Earlier in his career, he served as Group Commander and Captain of the Port for Long Island Sound in Long Island, New York.
Statement by Homeland Security Secretary Michael Chertoff:
http://www.dhs.gov/dhspublic/display?content=5355
Source: http://www.whitehouse.gov/news/releases/2006/01/20060119−3.h tml

34. *January 18, Federal Computer Week* — **DoD sets real−world test of HSPD−12.** An exercise to uncover operational problems in issuing and using uniform federal identity cards will begin

in April, Department of Defense (DoD) officials in charge of the project said on Wednesday, January 18. The exercise, involving 10 DoD sites and each military service, will test the requirements for Homeland Security Presidential Directive 12 (HSPD−12), said Bob Gilson, a management and program analyst. Officials who spoke on Wednesday at a Government Smart Card Interagency Advisory Board meeting in Washington, DC, alluded to the October 27 deadline for federal agencies to begin issuing interoperable identity cards to federal employees and contractors. The cards will be used to improve security at federal facilities. The purpose of the exercise, scheduled to last 287 days, is to find and correct real−world problems with using 64K contactless smart cards for secure access to DoD facilities, Gilson said.
Source: http://www.fcw.com/article92001−01−18−06−Web

[Return to top]

Emergency Services Sector

35. *January 18, Utica Observer−Dispatch (NY)* — **New York preparedness center to get $4.5 million.** New York Governor George E. Pataki plans to provide $4.5 million to the New York State Preparedness Training Center, which will be the first state−level training facility in the nation. The money, designated to develop and staff the facility, is part of the governor's 2006−07 budget proposal. The center would start up at the Oneida County Airport in Whitestown, NY, sometime in the middle of the year. Pataki announced in December the facility will train as many as 600 people a week and create about 36 jobs, though that number is expected to grow. "What this [funding] means is that the governor is giving us sufficient resources to complete the first phase of the training center," said Dennis Michalski, a spokesperson for the state Emergency Management Office. The $4.5 million is the first phase toward a $6 million total allotment for the center, said Scott Reif, a spokesperson for the governor's budget division. The state announced in December that first responders will learn how to handle chemical, biological, radiological, nuclear and explosive emergency situations through classroom and live training. One of the first classroom sessions in 2006 will educate trainees on weapons of mass destruction.
Source: http://www.uticaod.com/apps/pbcs.dll/article?AID=/20060118/NEWS/601180316/1001

36. *January 17, KOLD News 13 (AZ)* — **Arizona cities not ready to give government plan for emergency mass evacuation.** As a lesson learned from the gulf coast hurricanes, the federal government wants Tucson, AZ, and other major cities to have a plan for mass evacuation. A memo from the Department of Homeland Security calls on 75 of the nation's largest cities to have in place plans for complete evacuations of their residents. That plan was due Tuesday, January 17. Tucson, along with Phoenix and Mesa, are saying to the federal government "we're not going to give you a plan." The reason: there is no major disaster that would cause a need to evacuate all of Tucson. Disaster planners in Tucson, Phoenix and Mesa say they would be more likely receive evacuees from other cities. While Tucson doesn't have a plan to evacuate everyone, emergency responders from throughout the metro area have been working on planning for major disasters. They've identified the top four major hazards that could threaten the Tucson community. Tucson is asking the federal government to come up with hundreds of thousands of dollars for consulting; that is if homeland security still insists on a mass evacuation plan.

Source: http://www.kold.com/Global/story.asp?S=4374708&nav=14RT

[Return to top]

Information Technology and Telecommunications Sector

37. *January 18, Cisco Systems* — **Cisco CallManager denial of service.** Vulnerable versions of Cisco CallManager do not manage TCP connections and Windows messages aggressively, leaving some well known, published ports vulnerable to denial of service attacks. CallManager does not time out TCP connections to port 2000 aggressively enough, leading to a scenario where memory and CPU resources are consumed with enough open connections. In specific scenarios, CallManager will leave the TCP connection open indefinitely until either the CallManager service is restarted or the server is rebooted.
Source: http://www.cisco.com/warp/public/707/cisco−sa−20060118−ccmdo s.shtml

38. *January 18, Information Week* — **New worm hits the top of the threat charts.** A worm that debuted Tuesday, January 17, had quickly climbed the malware chart to the number three spot by Wednesday, January 18, a Finnish security company said. With a variety of names −− F−Secure calls it VB.bi, Symantec dubs it Blackmal.e, McAfee labels it MyWife.d −− the worm, said Helsinki−based F−Secure, is a simple Visual Basic (VB) construction that arrives as an e−mail file attachment. The worm also spreads through shared folders, and when activated tries to disable a number of security programs, including those sold by Symantec, McAfee, Trend Micro, and Kaspersky Labs. One of its distinguishing features, noted the Internet Storm Center (ISC) in its alert is that "the attachment can be either an executable file or a MIME file that contains an executable file." The latter tactic is meant to conceal the payload's danger; the MIME format is rarely used by attackers. One of the last great MIME−based attacks was the Nimda worm of 2001. Symantec, which tagged the worm with a "2" in its 1 through 5 threat scale, has posted a free−of−charge removal tool on its Website that deletes all traces of the malware.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=177101528

39. *January 18, Associated Press* — **Suspect in federal spam case pleads guilty.** The main defendant in America's first prosecution under a 2004 federal anti−spam law pleaded guilty Tuesday, January 17, to three felony charges, federal prosecutors said. Daniel J. Lin of West Bloomfield Township, MI, faces nearly five years in prison and a fine of up to $250,000, the U.S. Attorney's Office in Detroit said. Two of the counts are fraud charges involving millions of unsolicited spam e−mails sent to computer users. The other is possession of a firearm by a felon, for guns discovered when authorities raided Lin's suburban Detroit home. He is scheduled to be sentenced May 16 in U.S. District Court in Ann Arbor, MI. Lin and three other West Bloomfield Township men were identified in court documents as being part of the massive illegal spam scheme. Court papers described a complex web of corporate identities, bank accounts and electronic storefronts used to send hundreds of thousands of e−mail sales pitches for fraudulent products. The Federal Trade Commission said angry consumers forwarded to authorities more than 490,000 e−mails from the operation from January 2004 to April 2004 −− more than from any other spam outfit worldwide during the same period.
Source: http://www.cnn.com/2006/TECH/internet/01/18/internet.spam.ap /index.html

40. *January 18, Tech Web* — **Oracle fixes 82 database, server flaws.** Oracle on Tuesday, January 17, patched 82 different vulnerabilities in its flagship database and other server products, leading security company Symantec to raise the overall Internet threat status and others puzzling over the exact extent of the risk. The Critical Patch Update fixes 37 flaws in Oracle's Database, 17 in its Application Server, 20 in the Collaboration Suite, 27 in E−Business Suite, and one each in the PeopleSoft Enterprise Portal and JD Edwards HTML Server. While the number may seem staggering to those not used to Oracle's quarterly security updates −− Windows users, for instance, go into shock when Microsoft releases more than a dozen fixes in a given month −− January's batch is actually smaller than the October 2005 bunch. Then, Oracle patched 106 different bugs. Many of this quarter's fixed vulnerabilities were tagged by Oracle with its highest risk ratings −− unlike other vendors such as Microsoft, Oracle breaks out risk rankings into numerous sub−categories −− with notes that they're easy to exploit and have a potentially wide range of impact. Among the bugs are many which can be exploited remotely, and 61 which can be used by anonymous (non−authenticated) users.
Source: http://www.techweb.com/wire/security/177101585;jsessionid=VAJPECC3JG220QSNDBGCKHSCJUMEKJVN

41. *January 18, Security Focus* — **Window XP update delayed until after Vista.** Microsoft will not release Windows XP Service Pack 3 until the second half of 2007, after the company's planned shipment date for its next−generation operating system Vista, the software giant said on Wednesday, January 18. Vista will add some long−overdue security features, including limiting the privileges of the everyday user account similar to Unix−based systems, such as Linux and the Mac OS X. Another security feature that Microsoft touted −− the next−generation secure computing base (NGSCB), formally known as "Palladium" −− will only be partially incorporated in Vista, and it's uncertain whether it will follow the industry−created standard. The last major update for Windows XP, known as Service Pack 2, was released in August 2004 and added a host of new security features and bug fixes to Microsoft's flagship desktop operating system. Vista's focus on security will not eradicate security flaws −− just this week the software giant released an update for the beta version of the operating system to fix the recent vulnerability in the Windows Meta File (WMF) format.
Source: http://www.securityfocus.com/brief/107

42. *January 18, Government Computer News* — **Department of Homeland Security grant kit offers cybersecurity guidance.** The Department of Homeland Security's (DHS) new preparedness unit is urging state governors to prepare cybersecurity plans, adopt a new national XML−based model for information−sharing and implement newly developed common rules for geospatial content. The recommendations are some of the most detailed that the federal government has made to state and local governments on using IT in the fight against terrorism. The IT−related guidance is included in the fiscal 2006 grant application kit for the distribution of $3.9 billion in federal homeland security grants to states and localities this year, published by the preparedness directorate. Cybersecurity guidance was attached as an appendix for the first time. Guidelines for topics to be included in the cyberplans are somewhat open−ended. Recommendations cover about two−dozen questions related to policy, training, IT deployment and vulnerability. In addition, DHS is recommending that states, local and tribal government adopt geospatial data guidelines developed by the Information Content Subgroup of the Federal Geographic Data Committee Homeland Security Working Group in October 2005.
Source: http://www.gcn.com/vol1_no1/daily−updates/38026−1.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a public exploit for a vulnerability in VERITAS NetBackup Volume Manager Daemon (vmd). The VERITAS NetBackup vmd listens on network port 13701/tcp. An attacker could send a specially crafted packet to the Volume Manager on a vulnerable system to cause a buffer overflow or a denial of service condition. Successful exploitation may allow may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system with root or SYSTEM privileges. More information about this vulnerability can be found in the following URL:

VU#574662 VERITAS NetBackup library buffer overflow vulnerability:
http://www.kb.cert.org/vuls/id/574662

US−CERT strongly encourages users and administrators to review the following mitigation to address this vulnerability as soon as possible:

Review the Symantec Advisory SYM05−024 and apply the recommended updates to address this vulnerability:

http://seer.support.veritas.com/docs/279553.htm

http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNL OAD.htm

Restrict access to the ports used by the NetBackup services.

Malicious Website Exploiting Sun Java Plug−in Vulnerability US−CERT is aware of an active malicious website that exploits a vulnerability in the Sun Java JRE. The initial report led US−CERT to believe the website was exploiting VU#974188. After further analysis, it was determined that the actual vulnerability being exploited was VU#760344. This vulnerability allows a Java Applet to bypass java security settings. Once these checks are bypassed, a remote attacker may be able to exploit this vulnerability to execute arbitrary code on the host machine. More information about these vulnerabilities can be found in the following URL:

VU#760344 Sun Java Plug−in fails to restrict access to private Java packages:
http://www.kb.cert.org/vuls/id/760344

VU#974188 Sun Java Runtime Environment "reflection" API privilege elevation vulnerabilities: http://www.kb.cert.org/vuls/id/974188

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 139 (netbios−ssn), 25 (smtp), 135 (epmap), 7008 (afs3−update), 41170 (−−−), 6346 (gnutella−svc), 80 (www) 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

43. *January 19, Washington Post* — **Federal grants bring surveillance cameras to small towns.** Using federal grant money, Bellows Fall, VT, police plan to put up 24−hour cameras at such spots as intersections, a sewage plant, and the town square. Similar cameras are already up in the Virginia communities of Galax and Tazewell, where police can pan right down Main Street, and in tiny Preston, MD, with two police officers and five police cameras. An interest in public, permanent video surveillance is flowing down to the smallest levels of American law enforcement. Town size varies from Salisbury, MD, with 88 officers, which plans to put up seven cameras this year, to the Hoopa Valley Tribal Police in Northern California, where the nine−member force often has no officer on duty from 4 to 8 a.m. PST. In several cases, funding to buy cameras has come from the federal government, either for community policing or homeland security. Large police departments have only started to embrace public surveillance in the past six years or so, long after privately owned cameras became ubiquitous at banks, ATMs, and stores.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/18/AR2006011802324.html?sub=AR

[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