Department of Homeland Security Daily Open Source Infrastructure Report for 13 February 2007

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- Johns Hopkins –– which comprises Johns Hopkins University and Johns Hopkins Hospital in Baltimore –– disclosed that it has lost the personal data on roughly 52,000 employees and 83,000 patients. (See item 10)

- The U.S. Postal Inspection Service is working with law enforcement agents from the FBI and ATF, as well as local and state agencies, to investigate two explosive devices sent to financial institutions since January 31, and has its own employees nationwide on high alert to identify suspicious packages. (See item 14)

- The Associated Press reports thousands of people were evacuated from a Spokane mall Sunday afternoon, February 11, after noxious fumes of unknown origin sickened people inside. (See item 34)

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. *February 10, Cape Cod Times (MA)* — **NRC approves reduced safety staff at Pilgrim Nuclear Power Station.** Only one radiation protection technician needs to be on duty at any one time at the Pilgrim Nuclear Power Station in Plymouth, MA, Nuclear Regulatory

Commission (NRC) officials decided last week. Having only one of these technicians on duty at a time is typical of most other nuclear power plants, according to NRC regulations. The NRC also approved the first phase of heightened security measures for all nuclear plants last month. The new rule will put security changes implemented after the September 11 attacks in place permanently. It will increase the number of security guards on duty at all plants from three to five to protect against ground attacks.
Source: http://www.capecodonline.com/cctimes/nrcoks10.htm

2. *February 09, Platts Energy Bulletin* — **Nevada gas seen doubling by 2025; power sector to lead growth.** Nevada's natural gas use is expected to grow by about 3.4 percent a year and will likely double to 400 Bcf in 2025 from the 200 Bcf the state used in 2005, according to a study commissioned by state regulators. About 75 percent of the growth will come from natural gas−fired power plants, Arlington, VA−based Energy and Environmental Analysis told the Nevada Public Utilities Commission last week. Gas−fired generation in the state doubled to 5.7 GW from 2000 to 2005, and is expected to peak at 8 GW by 2010. As gas use rises, Nevada will need additional supplies, possibly from additional capacity on existing pipelines. "EEA estimates that [Nevada's] consumers will continue to rely on transport from the Kern River, El Paso, Transwestern, Tuscarora, and Paiute pipelines," the study said.
Source: http://www.platts.com/Natural%20Gas/News/6352718.xml?sub=Natural%20Gas&p=Natural%20Gas/News

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *February 12, Courier Herald (GA)* — **Odor leads to Hazmat investigation.** An unknown substance created havoc for a while at H&H Tire Saturday morning, February 10, in Dublin, GA. Owner Bucky Hobbs said when he arrived at work Saturday he noticed a strong odor he could not recognize and he called the authorities. “He called the fire department when his employees’ eyes began to burn,” said Dublin Police Chief Wayne Cain. “The fire department arrived on scene and had a similar reaction so to be on the safe side they called in the Hazmat team.” Cain said a powdery substance was located that was “partially identified and was cleared not to be toxic and not to be corrosive.” Dublin Police, Dublin Fire, Laurens County Emergency Management Agency Hazardous Materials Team and the Georgia Bureau of Investigation all responded and roped off the block keeping onlookers at a safe distance until the substance could be located and identified.
Source: http://news.mywebpal.com/news_tool_v2.cfm?pnpID=909&NewsID=782661&CategoryID=13280&show=localnews&om=1

4. *February 10, NBC 10 (PA)* — **Homes evacuated near oil refinery leak.** Residents have been given the all clear to return to 15 homes situated across the street from a ConocoPhillips in Trainer, PA, after a small gas leak. Company officials said the flammable gas is similar to propane used in backyard barbecue grills, and it never really threatened neighbor safety. "We had a leak of a light hydrocarbon product into our internal refinery storm water sewer system," said Bill Tyson, a spokesperson for ConocoPhillips. The evacuations were apparently voluntary and occurred on the block right across the street from the refinery, located at Post Road and Gilbert Street just outside of Chester. Shelter was set up for a time at the Marcus Hook Fire

Dept.'s Station 68, located at East 10th Street and Penn Avenue.
Source: http://www.nbc10.com/news/10980784/detail.html

[Return to top]

Defense Industrial Base Sector

5. *February 12, Federal Computer Week* — **DISA budgets $205.2 million for NCES over three years.** The Defense Information Systems Agency (DISA) has budgeted more than $200 million for its Net−Centric Enterprise Services (NCES) program over the next three years, with more than half of the spending planned for fiscal 2009. DISA said it plans to use NCES to build interfaces between incompatible systems and networks across the Department of Defense (DoD). The initiative will use metadata tagging, Web discovery, search and collaboration tools to make data visible to a wide range of DoD users. The agency has budgeted $143.9 million for NCES operations and maintenance over the next three years, including $86.9 million in fiscal 2009. The procurement budget over the same period is $60.4 million, with $28.9 million already budgeted for the 2007 fiscal year and planned spending of $10.8 million in 2008 and $20.7 million in 2009. DISA awarded its first NCES collaboration tool contract in July 2006 and plans to award a second contract this June.
Source: http://www.fcw.com/article97644−02−12−07−Web

6. *February 09, U.S. Army* — **Supplemental funds critical to Army readiness, officials say.** The Army is the best equipped, trained and led force it's ever been, but it needs continued funding to ensure it's ready to face future conflicts, the Army's top two leaders said in congressional testimony Friday, February 9. The fiscal 2007 war on terror supplemental funding request included in President Bush's budget is critical to improving breadth and depth of Army readiness, specifically in preparing units for deployment, Army Secretary Francis J. Harvey said at a hearing of the House Appropriations Committee's subcommittee on defense. "The solution to establishing the required breadth and depth of Army readiness ultimately rests in providing the required resources," Harvey said. "That in turn results in an Army force structure that can meet the current and projected operational demand." One of the issues highlighted by Harvey and Army Gen. Peter J. Schoomaker, Army chief of staff, who also was at the hearing, was the equipment shortage for units in the U.S. The Army went into this war with an equipment shortage, and has since been growing the force, so that shortage has become even larger, Schoomaker pointed out.
Source: http://www.army.mil/−news/2007/02/09/1796−supplemental−funds−critical−to−army−readiness−officials−say/

[Return to top]

Banking and Finance Sector

7. *February 12, Reuters* — **Mobile carriers to make it easy to send money home.** Mobile communications operators and banks joined forces on Monday, February 12, to make it easier and cheaper for hundreds of millions of immigrants and migrant workers to send money home by using their mobile phones. The aim is to reduce the transaction costs of sending small

amounts of cash to just a few percent, from a current 24 percent for amounts as small as $50. A group of 19 mobile operators with networks in over 100 countries and representing over 600 million customers will create a global system that could double the number of recipients of international remittances to more than 1.5 billion, while helping to quadruple the size of the remittances market to more than $1 trillion by 2012. Mobile operators are partnering with banks at a local or regional level. The idea is that people can load cash on their mobile, and order it to be sent to a mobile phone number in another country, where the recipient receives a message that money has arrived, making it as easy as sending a text message.
Source: http://www.reuters.com/article/technologyNews/idUSL093130272 0070212

8. *February 11, Associated Press* — **Data breech may affect thousands of Washington Metropolitan Police Department officers.** Personal information has been accidentally released about some Washington, DC, police officers, including their Social Security numbers. A letter has gone out from the District Chief Financial Officer to notify nearly 2,000 members of the Metropolitan Police Department who may be affected. It says the information was inadvertently released to two Advisory Neighborhood Commission officials who had requested information about police overtime. The letter from the CFO's office says they are taking the issue seriously but believe the risk of identity theft or other problems is minimal. It says the Social Security numbers have been erased from the computers of those who were given the information. The city CFO is offering a year of free credit monitoring for those who were affected.
Source: http://www.wusa9.com/news/news_article.aspx?storyid=55776

9. *February 10, Journal Gazette (IN)* — **Hacker gets credit card info from Indiana state Website.** State technology officials sent letters Friday, February 9, to 5,600 people and businesses informing them that a hacker obtained thousands of credit card numbers from the state Website. Although numbers are usually encrypted or shortened to the last four digits, the Office of Technology conceded a technical error allowed the full credit card numbers to remain on the system and be viewed by the intruder. Chris Cotterill, director of the site, www.IN.gov, said the hacking occurred in early January but wasn’t discovered until January 25. The state has already notified the Secret Service and the credit card companies of those cards that were viewed. Each account has been placed on a watch list to track potential fraudulent activity. None has been apparent so far. All three consumer reporting agencies have been contacted, and the affected cardholders were asked to review their credit card statements since January 1. He said the state Website offers more than 300 online services and has been conducting online transactions for about a decade.
Source: http://www.fortwayne.com/mld/journalgazette/16667910.htm

10. *February 09, InformationWeek* — **Johns Hopkins loses data on 130,000 patients, employees.** Johns Hopkins disclosed this week that it has lost the personal data on roughly 52,000 employees and 83,000 patients. The Maryland−based organization, which comprises Johns Hopkins University and Johns Hopkins Hospital, has reported that nine backup computer tapes were not returned from a contractor, which routinely takes them and makes microfiche backups of them. Eight of the tapes, according to a notice on Johns Hopkins Website, contain "sensitive" personal information on employees, and a ninth tape contains "less sensitive" personal information on the hospital's patients. Johns Hopkins says it has no evidence that the tapes were stolen or that the information on them has been misused. The statement also calls the risk of

identity theft "very, very low." "Our best information is that the tapes have been destroyed," said William R. Brody, president of Johns Hopkins University. Letters are being sent to all affected Johns Hopkins University employees, current and former, and to all affected Johns Hopkins Hospital patients with available addresses.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=GCBBKMAVFGRDWQSNDLRCKH0CJUNN2JVN?articleID=197004916&articleID=197004916

[Return to top]

Transportation and Border Security Sector

11. *February 12, Christian Science Monitor* — **Asia's discount airlines reach for the West.** Spurred by open−skies policies and booming tourism, low−cost airlines are mushrooming across Asia. Most have adopted the business model pioneered in the 1970s by Southwest Airlines −− lean, mean, and affordable −− to fly budget−conscious passengers around the region. Now airline entrepreneurs are setting their sights on more distant destinations, betting that long−haul travel is equally ripe for discounting. Oasis, a start−up airline in Hong Kong, has begun daily flights to London for as low as $147 one way and plans this year to offer similar deals to Oakland, CA, and Chicago. Jetstar Airways, a subsidiary of Australia's Qantas Airways, sells bargain tickets on routes between Australia and Southeast Asia. And Malaysia's AirAsia, the largest budget airline in Asia, recently founded a new operator, AirAsiaX, to ply long−haul routes to China and Britain starting in July. Creating long−haul budget airlines that can take on the state−run carriers that dominate in Asia could prove more challenging, though. So how can they keep fares so low? The secret, says Steve Miller, CEO of Oasis, lies in the efficient use of aircraft and crews, flexible pricing, and an attractive business class.
Source: http://www.csmonitor.com/2007/0207/p06s02−woap.html

12. *February 12, Canada Press* — **Day: Air security improving.** Transport Canada is moving "aggressively" on a report from the global aviation authority that calls for beefed up air security through improved cargo screening and better training programs, Public Safety Minister Stockwell Day said Monday, February 12. Day's comments follow a published report that revealed portions of a confidential audit handed to Transport Canada by the International Civil Aviation Organization, a UN agency based in Montreal. The audit team reviewed a range of security−related issues concerning airports, including passengers, baggage, in−flight measures, cargo and catering services. Transport Canada has called the report "a valuable tool." The report echoes the recent concerns of an advisory panel struck by the Canadian Air Transport Security Authority, a federal agency created after 9/11 to make the air travel safer. Air security has been a major preoccupation for policy−makers since terrorists hijacked passenger jets and crashed them into the World Trade Center and Pentagon in 2001. The panel recommended Transport Canada "accelerate its work" to develop a program for the security screening of aviation cargo.
Source: http://cnews.canoe.ca/CNEWS/War_Terror/2007/02/12/3597019−cp .html

13. *February 12, WNYC (NY)* — **Officials gather to discuss train gaps.** Railroad officials from across the U.S. will meet this week to discuss federal standards for train platform gaps. The Federal Railroad Administration's General Passenger Safety Task Force meets Tuesday, February 13, and Wednesday, February 14, and will discuss platform gaps. The national task

force intends to publish a study on platforms level with train doors. It could also propose federal regulations. There are currently no national standards for platform gap size.
Source: http://www.wnyc.org/news/articles/73521

[Return to top]

Postal and Shipping Sector

14. *February 10, USPS News Release* — **Post offices on high alert for suspicious packages.** The U.S. Postal Inspection Service is working with law enforcement agents from the FBI and ATF, as well as local and state agencies, to investigate two explosive devices sent to financial institutions since January 31. While the investigation continues, Postal Inspectors are encouraging the financial industry to re−examine their procedures for handling correspondence and packages. The U.S. Postal Service (USPS) has its employees nationwide on high alert to identify suspicious packages; they receive training in the identification and proper handling procedures for packages that may be hazardous or dangerous. Keeping the mail safe is and will continue to be the highest priority of the U.S. Postal Service and U.S. Postal Inspection Service. To obtain the poster on identifying suspicious packages and reporting them to authorities: to http://www.usps.com/postalinspectors/pos84.pdf or contact any local post office.
Source: http://www.usps.com/communications/newsroom/2007/pr07_is0210 .htm

[Return to top]

Agriculture Sector

15. *February 12, Associated Press* — **Wild pigs bring pseudorabies to Platte County.** Wild pigs have brought a swine disease that can devastate pork operations to Platte County in central Nebraska, the state Department of Agriculture said. The sow and nine piglets, likely hybrids of domestic hogs and Eurasian wild boars, were killed by the Nebraska Game and Parks Commission. Tests of the pigs revealed pseudorabies, a contagious viral disease that mostly affects swine, although cattle, sheep, dogs and cats also can be infected.
Source: http://www.yorknewstimes.com/stories/021207/ag_wildpigs.shtm l

16. *February 07, WorldPoultryNet* — **Birds culled due to Salmonella.** In what is believed to be the country's biggest salmonella outbreak in poultry in 10 years, authorities in southern Sweden cull over 100,000 chickens. Birds at seven farms in southern Sweden were tested positive for salmonella, resulting in slaughtering. The source of the outbreak is unclear, but it is believed the bacteria could have spread from infected mice or rats, or through the feed.
Source: http://www.worldpoultry.net/ts_wo/worldpoultry.portal/enc/_n fpb/true/tswo_portlet_news_singleeditorschoice1_3_actionOver ride/___2Fportlets___2Fts___2Fge___2Fnews_singleeditorschoic e1___2Fcontent___2FshowDetailsList/_windowLabel/tswo_portlet _news_singleeditorschoice1_3/tswo_portlet_news_singleeditors choice1_3id/12525/_desktopLabel/worldpoultry/_pageLabel/tswo__page_news_content/

[Return to top]

Food Sector

17. *February 12, Canadian Press* — **Doctored baby formula prompts health warning.** Canada's food agency issued a public warning after two cans of powdered baby formula were found to have been tampered with at a Zellers store in Saskatoon. Police and the Canadian Food Inspection Agency are investigating after the half−empty cans of Enfamil−brand formula were found to have puncture holes, which were concealed by the product label.
Source: http://www.theglobeandmail.com/servlet/story/LAC.20070212.NATS12−3/TPStory/National

[Return to top]

Water Sector

18. *February 11, Associated Press* — **Sierra Nevada towns worry about water contamination.** Water from two wells in California's Sierra Nevada town of East Orosi contains dangerous levels of a banned pesticide and nitrates from fertilizers, septic tanks and sewage plants. Cutler, next door to East Orosi, is under a state order to clean up nitrates in the town's drinking water. Contaminants have been found in wells in Woodlake, Lemon Cove, Tooleville, Woodville and Yettem. A state study last year revealed that 75 wells in Tulare County had nitrate contamination, or about two of every five private wells tested. Yuba, El Dorado and Tehama counties had a combined total of 11 wells with high nitrate levels.
Source: http://www.signonsandiego.com/news/state/20070211−1500−ca−brf−norcal−contaminatedwater.html

[Return to top]

Public Health Sector

19. *February 12, Reuters* — **Most bird flu victims under forty.** Ninety percent of the people infected with bird flu have been under the age of 40, and 60 percent of them have died, according to the latest analysis from the World Health Organization (WHO). But the WHO researchers stressed their analysis did not suggest why this might be and noted there are several theories on why the H5N1 virus seems to attack younger people. The analysis said the median age of people confirmed infected was 18 years old and ranged from three months to 75 years. Just over half of all cases (52 percent or 132 out of 256) were aged under 20 years, and 89 percent were aged under 40 years. The WHO researchers found that H5N1 has killed 60 percent of its victims and found big differences in fatality by age. The highest case fatality rate (76 percent) was found among those aged 10 to 19 years; the lowest case fatality rate (40 percent) was found among those aged over 50 years. Bird flu killed 44 percent of victims under the age of five and 66 percent of those aged 30 to 39.
Source: http://in.today.reuters.com/news/newsArticle.aspx?type=worldNews&storyID=2007−02−12T071042Z_01_NOOTR_RTRJONC_0_India−287 257−1.xml

20.

February 12, Associated Press — **FDA restricts use of antibiotic.** The U.S. government on Monday, February 12, restricted use of an antibiotic linked to rare reports of severe liver problems, including several deaths, saying the drug now should be used only to treat pneumonia but not less serious bacterial infections like bronchitis and sinusitis. The U.S. Food and Drug Administration (FDA) said the antibiotic, Ketek, would remain on the market but that its label will bear a new, stern warning. The agency said it and manufacturer also created a guide for patients outlining the drug's risks and its safe use. As of late last year, doctors had prescribed the antibiotic more than 5.6 million times in the U.S. since it won FDA approval in 2004.
Source: http://www.msnbc.msn.com/id/17115795/

21. *February 12, Agence France−Presse* — **Four Turkish villages quarantined over bird flu fear.** Four more villages in southeastern Turkey have been quarantined over bird flu fears after the presence of the H5N1 virus was confirmed last week in the region. The village of Akcay and three nearby hamlets in the mainly Kurdish province of Diyarbakir were placed under quarantine following the deaths of poultry there, said the head of the local agriculture department, Mustafa Kayhan. "There is a suspicion of bird flu," he said, adding that samples from dead birds were sent to a laboratory for analyses Monday, February 12. The H5N1 virus, which claimed four lives in Turkey a year ago, resurfaced last week in the village of Bogazkoy in the neighboring province of Batman.
Source: http://news.yahoo.com/s/afp/20070212/hl_afp/healthfluturkey_070212150107;_ylt=AqIYUJCEJlb3DYYR4kXLpPiJOrgF

22. *February 12, SAPA (South Africa)* — **Extreme drug resistant tuberculosis found in all provinces.** Extreme drug resistant tuberculosis (XDR−TB) can be traced to all provinces, the South African health department said on Monday, February 12. "All provinces have been able to trace cases of XDR−TB," the department said of a lethal form of the infectious disease which first emerged in the Tugela Ferry region of KwaZulu−Natal two years ago. Health spokesperson Sibani Mngadi said 269 cases of XDR−TB had been recorded nationally. The health department issued the statement in response to drastic new measures proposed by the Johannesburg−based Public Library of Science −− including infection monitoring at airports and border posts and the isolation of patients, even against their will −− to prevent the spread of XDR−TB. This came amid conflicting reports of how many people had died in the Eastern Cape from the disease. Figures released by the Johannesburg−based National TB Control Unit last week put the death toll from XDR−TB at 183 nationally since it was identified in September last year. The unit said some 328 cases of XDR−TB had been identified and added that its own figure showed that some 18 people had died from the disease in the Eastern Cape.
XDR−TB information: http://www.cdc.gov/nchstp/tb/default.htm
Source: http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=nw20070212182424135C137232

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

23. *February 11, Associated Press* — **Japan uses satellites to track disasters.** Japan launched a satellite−based alert system Friday, February 9, that will instantly send warnings of tsunamis and updates on volcanic activity to help speed evacuations, an emergency official said. Under the system, called "J−ALERT," the nation's Fire and Disaster Management Agency will immediately transmit warnings on tsunamis if an earthquake occurs. It will also issue alerts following signs of volcanic activity based on information from the Meteorological Agency to local authorities, said Fire and Disaster Management agency spokesperson Takeshi Itoh. Information on strong earthquakes after they occur will also be sent, Itoh said. The warnings will activate communication devices in the regions connected to the system, setting off sirens and voice advisories via radio, Itoh said.
Source: http://www.forbes.com/feeds/ap/2007/02/11/ap3416268.html

24. *February 11, Associated Press* — **New York City to try multimedia 911.** New York City wants to broaden the 911 system to accept digital photos and video clips of accidents and crimes. But the expansion of the massive 911 system, which already handles roughly 11 million calls a year, raises questions about what to do with all that data. City officials say they're not worried about their ability to process all the digital images −− or the possibility that hoaxes might trip up dispatchers. The New York initiative, announced in January, will involve equipping 911 facilities with the necessary technology to accept the photos and videos, which often may come from individuals' cell phones. The city also intends to upgrade its non−emergency services through the 311 information hot line, which gets about 14.6 million calls a year. In adding image capability, New York City will be at the forefront of governments upgrading emergency−response systems to take advantage of the wireless age, joining states such as Indiana, Tennessee and Vermont in working to enhance their systems.
Source: http://www.contracostatimes.com/mld/cctimes/news/local/states/california/16675786.htm

25. *February 09, Federal Emergency Management Agency* — **President declares major disaster for Illinois.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) Friday, February 9, announced that federal disaster aid has been made available for Illinois to supplement state and local recovery efforts in the area struck by a severe winter storm from November 30 to December 1, 2006. FEMA Director David Paulison said federal funding is available to State and eligible local governments and certain private nonprofit organizations on a cost−sharing basis for emergency work and the repair or replacement of facilities damaged by the severe winter storm in the counties of Bond, Calhoun, Christian, DeWitt, Fayette, Jersey, Logan, Macon, Macoupin, Madison, McLean, Monroe, Montgomery, Piatt, Sangamon, Shelby, St. Clair, and Woodford.
Source: http://www.fema.gov/news/newsrelease.fema?id=34066

[Return to top]

Information Technology and Telecommunications Sector

26. *February 12, IDG News Service* — **China and Russia top list of worst copyright violators.** China and Russia are the two worst foreign infringers of U.S. software and music copyrights and they should remain on the U.S. government's priority watch list, a group representing the software, music, books, and movie industries said Monday, February 12. The International Intellectual Property Alliance (IIPA) put out the figures as part of its recommendations to the U.S. Trade Representative. China topped all rivals on the IIPA most−wanted list by pumping out $2.21 billion worth of pirated goods last year, mainly business software, according to IIPA figures. Russia ran a close second at $2.18 billion, it said.
Source: http://www.infoworld.com/article/07/02/12/HNworstcopyrightvi olators_1.html

27. *February 12, InformationWeek* — **Penn State researchers develop new worm−stopping technology.** Researchers at Penn State University say they have developed anti−malware technology that can identify and contain worms in milliseconds rather than minutes −− greatly limiting how far they spread and how much damage they cause. The new technology focuses on analyzing packet rate and frequency of connections, rather than signature or pattern identification, according to a release from Penn State. "A lot of worms need to spread quickly in order to do the most damage, so our software looks for anomalies in the rate and diversity of connection requests going out of hosts," said Peng Liu, associate professor of information sciences and technology at Penn State and lead researcher on the system. Penn State researchers assert that because many security technologies focus on signature or pattern identification for blocking worms, they cannot respond to new attacks fast enough, allowing worms to exploit network vulnerabilities.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=
MIRYBBI1UOICGQSNDLRCKH0CJUNN2JVN?articleID=197005266

28. *February 12, InformationWeek* — **SANS warns of 'major zero−day' bug in Solaris.** The SANS Institute is warning of a zero−day bug in Sun's Solaris 10 and 11 Telnet that allows hackers to easily gain remote access to the computes running the operating systems. The vulnerability −− called a "major zero−day bug" −− has been verified, according to a release on the SANS' Internet Storm Center Website. The problem lies in the way Telnet, which is a network protocol, uses parameters during the authentication process, says Johannes Ullrich, chief research officer at the SANS Institute and chief technology officer for the Storm Center. Ullrich says that by simply adding what he calls a "trick" or simple text to the telnet command, the system will skip asking for a user name and password. No exploit needs to be downloaded. Every Solaris 10 and 11 system is at risk. If the systems are installed out of the box, they automatically come Telnet enabled. Storm Center analysts are recommending that Telnet be disabled on the Solaris systems.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=
MIRYBBI1UOICGQSNDLRCKH0CJUNN2JVN?articleID=197005178

29. *February 12, Sophos* — **Valentine's spammers face a harder sell.** In the run−up to Valentine's Day, Sophos has reported seeing a rise in the number of spam campaigns selling romantic gifts such as jewelry, chocolate and lingerie. However, a new Sophos poll reveals that just five percent of computer users now admit to purchasing goods sold via spam, compared to nine percent this time last year. According to Sophos, many of the Valentine's Day themed campaigns make use of graphics embedded in the regular e−mail text. This type of image spam, most often used for promoting stock pump−and−dump scams or medication, is popular with

spammers thanks to its ability to bypass anti−spam filters that scan text content only.
Source: http://www.sophos.com/pressoffice/news/articles/2007/02/vale ntine.html

30. *February 09, Federal Computer Week* — **Attack by Korean hacker prompts DoD cyber debate.** The Department of Defense (DoD) computer networks are probed and attacked hundreds of time each day. But a recent attack on the civilian Internet is causing DoD officials to re−examine whether the policies under which they fight cyber battles are tying their hands. “This is an area where technology has outstripped our ability to make policy,” said Air Force Gen. Ronald Keys, Commander of Air Combat Command. “We need to have a debate and figure out how to defend ourselves.” Unlike in the war on terror, DoD can’t go after cyber attackers who plan or discuss crimes until they act, Keys said. Websites in other countries are beyond DoD's reach, he added. “If they’re not in the United States, you can’t touch 'em.” Keys said it would probably take a cyber version of the 9/11 attacks to make the U.S. realize that barriers to action in cyberspace should be re−evaluated.
Source: http://www.fcw.com/article97645−02−09−07−Web

31. *February 09, CNET News* — **Price of cybercrime tools shrinks.** It's becoming cheaper and easier to get hold of the tools needed to launch a cybercrime attack, according to security company RSA. Jens Hinrichsen, the company's product marketing manager for fraud auction, said Thursday, February 8, that RSA has been monitoring the Websites and ICQ channels where malicious hackers and cybercriminals interact. These sites allow participants to share feedback and even review one another's products. Addressing an audience at the RSA Conference 2007, Hinrichsen showed several screengrabs to illustrate that the prices being asked for hacking tools have been dropping, with many participants embracing volume discounts and other incentives. One example was a post offering a "Super Trojan," which could be used to install malicious code on a victim's PC, for $600.
Source: http://news.com.com/Price+of+cybercrime+tools+shrinks/2100−7349_3−6158025.html

Internet Alert Dashboard

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

32. *February 12, Associated Press* — **Hazmat scare in Richmond.** Hazardous materials teams were called to the state Supreme Court building Monday, February 12, after a worker opened an envelope containing a white, flaky substance, authorities said. The entrance to the Supreme Court was cordoned off by authorities and its ventilation system was shut down, but the offices were not evacuated. Capitol Police Chief Kim Lettner said the material from the envelope would be quickly tested for hazardous substances, such as anthrax, and then sent to a lab for

further testing.
Source: http://www.dailypress.com/news/local/virginia/dp−suspicioussubstance0212feb12,0,7952071.story?coll=dp−headlines−virginia

33. *February 12, Galesburg Register−Mail Online (IL)* — **Police investigating two works bomb explosions.** Galesburg, IL, police are investigating two works bomb explosions reported on Sunday, February 11. Investigating officers found remnants of two exploded works bombs and a live works bomb in the road in front of 228 Fulton St. A works bomb is a homemade bomb made from common household ingredients. Although these types of bombs do not cause flames or produce a tremendous amount of heat, they can cause burns or injury to the eyes of a person.
Source: http://www.register−mail.com/stories/021207/LOC_BCC8HDF7.GID .shtml

34. *February 11, Associated Press* — **Thousands flee fumes at Washington state mall.** Thousands of people were evacuated from a Spokane, WA, mall Sunday afternoon, February 11, after noxious fumes of unknown origin sickened people inside, fire officials said. At least 36 people in NorthTown Mall sought treatment at hospitals, Spokane police said. Police called the fumes a "possible chemical irritant," but still do not know what the irritant was. None of the conditions were considered life threatening, Fire Chief Bobby Williams said. Hazardous materials crews were investigating the cause of the fumes. Shoppers and mall employees were told it was either a gas leak or pepper spray. The mall was evacuated about 3:30 p.m. PST, and closed for the day.
Source: http://www.usatoday.com/news/nation/2007−02−11−wash−mall_x.h tm

[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

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.