Department of Homeland Security Daily Open Source Infrastructure Report for 27 February 2006

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

Daily Highlights

- Potomac News reports the Social Security Administration is warning people about a recent e−mail that asked for personal information through a link to a site that replicates a slightly altered version of its official Website. (See item 7)
- The Los Angeles Times reports Tennessee has ended its policy of issuing "certificates for driving" to illegal immigrants, citing federal investigations that uncovered applicants using fraudulent documents to obtain driving privileges. (See item 10)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

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

1. *February 24, Associated Press* — **U.S., Britain conduct nuclear experiment.** U.S. and British government scientists performed an underground nuclear experiment, short of a nuclear blast, at the Nevada Test Site on Tuesday, February 21, the National Nuclear Security Administration said. The experiment involved detonating high explosives around radioactive material at a desert testing range 85 miles northwest of Las Vegas, NV. No radioactivity was released in the subcritical experiment, said Nancy Tufano, spokesperson for Bechtel Nevada. Scientists for the first time posted a nearly eight−minute video Web log of preparations for the experiment. Tufano described the material tested as specially processed nuclear plutonium. The test was

designed to examine the effects of the explosion on the nuclear material. It was the 22nd subcritical test at the site since 1997. Federal officials call subcritical experiments essential to maintaining the safety and reliability of the U.S. nuclear arsenal.
Source: http://www.cbsnews.com/stories/2006/02/24/ap/tech/mainD8FV7I 08K.shtml

2. *February 23, Chicago Tribune (IL)* — **Exelon shuts down reactor.** Exelon Corp. has shut down its 912−megawatt Quad Cities 1 nuclear reactor in Illinois. According to Craig Nesbit, a spokesperson for Chicago−based Exelon on Wednesday, February 22, “There was an "electrical anomaly outside the plant.” The anomaly affected the main power transformer and idled the generator, which resulted in the reactor shutting down. Nesbit said the incident might have stemmed from the electrical grid or could have occurred in the plant's switchyard. He could not say when the plant may resume production. Quad Cities 1 is one of two units located in Cordova, IL. The other unit is operating at 85 percent of capacity, according to the Nuclear Regulatory Commission.
Source: http://www.chicagotribune.com/business/chi−0602230092feb23,1 ,4921765.story?coll=chi−business−hed&ctrack=1&cset=true

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *February 24, Aviation Week* — **Navy's No. 2 leader says service committed to 10 aircraft carrier air wings.** The U.S. Navy is committed to maintaining 10 aircraft carrier wings, according to Adm. Robert Willard, vice chief of naval operations. However, the Navy must overcome funding hurdles to keep those 10 wings adequately equipped in a time of budget constraints. Willard, a naval aviator and former aircraft carrier commander, notes that much of the Navy's F/A−18 fleet is aging and "we're trying to extend their life a bit to try and bridge the gap" until the Joint Strike Fighter comes on line in 2013 or 2014. The Navy is seeking funding in fiscal 2007 to replace 30 older F/A−18s with newer F/A−18Es and 18−Fs.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily _story.jsp?id=news/WING02246.xml

4. *February 23, Defense Industry Daily* — **India's Air Force looks to enhance its reach with upgrades and force multipliers.** India's Air Chief Marshal S.P. Tyagi's recently remarked that the Indian Air Force plans to acquire more advanced fighters, sophisticated defense systems and smart long−range weapons. Tyagi said the current scenario "necessitated a strategic reach to safeguard our national interests." Tyagoi acknowledged the effect that delays in the LCA Tejas fighter were having on India's force structure, but noted that India would react in a number of ways. One response, he said, would be to speed up the delivery of the 140 Su−30MKI jets. A second component of that response is to implement upgrade programs across India's fighter fleets. Another component is the induction of force multipliers like air tankers,

AWACS, and precision weapons.
Source: http://www.defenseindustrydaily.com/2006/02/indias−air−force −looks−to−enhance−its−reach−with−upgrades−force−multipliers/ index.php#more

[Return to top]

Banking and Finance Sector

5. *February 24, Fine Extra* — **One−fifth of bank branches in UK closed.** UK banks have closed one in five branches in the last ten years despite research showing that the majority of customers still prefer to do their banking at a branch. The study, which was sponsored by the Economic and Social Research Council, found that banks closed around 4,041 branches, and opened 1,074 between 1995 and 2003; a closure rate of 20 percent. The report shows that the highest rate of closure −− almost 24 percent −−occurred in less affluent inner cities and manufacturing areas. But despite the apparent closures, many high street banks claim they are actually investing in their branch networks rather than shutting them down. Barclays is currently undertaking a major revamp of 1,500 of its UK branches while others are introducing a number of new concept branches which are designed to encourage customers to use direct banking services in the branch. A study released by Forrester Research last year shows that over half of UK customers still visit a bank branch each month and British consumers are among the most frequent branch visitors in Europe, with 55 percent of customers surveyed visiting a branch monthly, mainly for routine tasks like depositing checks and withdrawing cash.
Source: http://finextra.com/fullstory.asp?id=14960

6. *February 23, Reuters* — **FTC settles with CardSystems over data breach.** A credit card processing company agreed to settle allegations that it failed to protect consumer data, resulting in millions of dollars in fraudulent purchases, the U.S. Federal Trade Commission (FTC) said on Thursday, February 23. The security breach by CardSystems Solutions Inc. is the "largest known compromise of financial data to date," the FTC said. The proposed settlement requires the company to adopt stricter security measures and have an independent audit every other year for the next 20 years. "CardSystems kept information it had no reason to keep and then stored it in a way that put consumers' financial information at risk," said Deborah Majoras, FTC chairperson. CardSystems authorized and approved credit and debit card purchases for merchants. Last year, it processed 210 million card purchases for 119,000 merchants. CardSystems collected card numbers and other data which was stored on its computer network. CardSystems was accused of failing to have enough security measures in place to keep hackers out of its computer network and to limit access between computers on its network and between its computers and the Internet. The lack of security "compromised millions of credit and debit cards, and led to millions of dollars in fraudulent purchases," the FTC said.
Source: http://www.eweek.com/article2/0,1759,1930716,00.asp?kc=EWRSS 03119TX1K0000594

7. *February 23, Potomac News (MD)* — **Fake Social Security site part of scam.** As consumers become savvier to such “phishing” scams, scammers are creating more complex ways of gaining personal information including bank account, Social Security and personal identification numbers. The Social Security Administration (SSA) is warning people about a

recent e−mail that asked for personal information through a link to a site that replicates a slightly altered version of its official Website. “What was unique about this situation was that when you clicked on the link, it took you to a clone of [SSA’s] Website,” said Mark Lassiter, SSA spokesperson. The government agency found out about the scam Friday, February 17 from people who were unsure if the e−mail was a legitimate request, Lassiter said. The e−mail in this case shared neither the www.ssa.gov or the www.socialsecurity.gov URL that Lassiter said are used to access the official Website. Social Security is not known to make many press releases, Lassiter said, but added that the severity of the situation warranted a quick turn−around. “We released the information within a couple hours of finding out,” he said.
Source: http://www.potomacnews.com/servlet/Satellite?pagename=WPN/MGArticle/WPN_BasicArticle&c=MGArticle&cid=1137834285869&path

8. *February 23, CNET News* — **Auditor loses McAfee employee data.** An external auditor lost a CD with information on thousands of current and former McAfee employees, putting them at risk of identity fraud. The disc was lost on December 15 by Deloitte & Touche USA, McAfee spokesperson Siobhan MacDermott said. She said the security software company was first notified on Wednesday, January 11. The disc contained personal details on all current U.S. and Canadian McAfee workers hired prior to April 2005 and on about 6,000 former employees in the same region, MacDermott said. The information wasn't encrypted and potentially includes names, Social Security numbers and stock holdings in McAfee. MacDermott said, "We have no reason to believe that any of the information has been accessed, and we are proactively protecting McAfee current and former employees with credit monitoring services." Deloitte & Touche confirmed the incident. A representative for the professional services firm said, "A Deloitte & Touche employee left an unlabelled backup CD in an airline seat pocket...We are not aware of any unauthorized access to this data in the two months since the CD was lost."
Source: http://news.com.com/Auditor+loses+McAfee+employee+data/2100−1029_3−6042544.html?tag=cd.lede

[Return to top]

Transportation and Border Security Sector

9. *February 25, Associated Press* — **Continental fights back with increased capacity.** Continental Airlines expects to expand route capacity in both the domestic and international markets this year, President Jeff Smisek said Thursday, February 23. Houston−based Continental expects overall capacity to rise at a time when most big airlines are cutting U.S. capacity, Smisek said. "A significant portion of our domestic growth is in response to incursion of low−cost carriers in our hub," Smisek said. Continental is focusing on returning to sustained profitability, Smisek said. The key for airlines is to emphasize margins ahead of per−passenger revenue or costs.
Source: http://www.usatoday.com/travel/flights/2006−02−24−continenta l−adding_x.htm

10. *February 25, Los Angeles Times* — **Tennessee ends cards for immigrant drivers.** Tennessee has ended its policy of issuing "certificates for driving" to illegal immigrants, citing federal investigations that uncovered applicants using fraudulent documents −− and even bribing state workers −− to obtain driving privileges, officials said Friday, February 24. The state began giving immigrants the certificates in July 2004, with the hope of balancing domestic security

and traffic concerns. The cards give holders the legal right to drive but, unlike driver's licenses, they are not to be used for identification purposes. For instance, they cannot be used to board an airplane. Officials in the capital, Nashville, grew concerned in recent months as federal investigations uncovered numerous instances of fraud by illegal immigrants. Bob Corney, a spokesperson for Tennessee's Democratic Gov. Phil Bredesen, said the governor's office was informed that immigrants were coming from other states to get the certificates, using forged residency documents. Last month, a former worker at a driver's license office was sentenced to two years in federal prison for issuing more than 40 certificates to unqualified immigrants, taking a $400 bribe for each fraudulent card.
Source: http://www.latimes.com/news/printedition/asection/la−na−drivers25feb25,1,2936821.story?coll=la−news−a_section

11. *February 23, Boston Globe* — **JetBlue, Southwest to raise air fares.** Two of the nation's leading low−cost airlines signaled on Wednesday, February 22, that they intend to raise fares this year, which could ease pressure on other airlines and allow them to also increase prices. "We need a higher average fare for our tickets," said David Neeleman, chief executive at JetBlue, which reported its first quarterly loss this month and is forecasting a loss for all of 2006. Laura Wright, chief financial officer at Southwest, said it's facing $600 million in higher fuel costs this year and will need to cover that expense. Terry Trippler, an airline specialist at Cheapseats.com , said the cost pressures that other airlines have been struggling with for years are finally starting to catch up with two of the leading low−cost carriers. The so−called legacy carriers such as American, United, Delta, Continental, and Northwest have had to cut their costs dramatically, often while in bankruptcy protection, to compete with discounters such as Southwest and JetBlue. Both have lower cost structures.
Source: http://www.boston.com/business/articles/2006/02/23/jetblue_southwest_to_raise_air_fares/

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

12. *February 26, Agence France−Presse* — **France fears outbreak of sheep disease.** France fears it might have an outbreak of a rare strain of "mad sheep" disease, the agriculture ministry has said. Two suspected cases of a rare strain of the brain−wasting disease, which is also called Scrapie, have been identified on two different farms in central France, the ministry said in a statement.
Scrapie information: http://www.aphis.usda.gov/vs/nahps/scrapie/
Source: http://news.yahoo.com/s/afp/20060226/hl_afp/healthfranceflusheep_060226162607;_ylt=AscGsrRUB9wujrSh8kE4r0GKOrgF;_ylu=X3oDMTA2ZGZwam4yBHNlYwNmYw−−

13. *February 24, Delta Farm Press* — **Hurricanes dealt $2.2 billion blow to Mississippi agriculture.** Agriculture in Mississippi is a $5.5 billion per year industry −− and Hurricanes Katrina and Rita wiped out nearly half of that, said Lester Spell, the state's commissioner of agriculture and commerce, at the Conservation Systems Cotton and Rice Conference. Among losses to the state's agriculture, Spell said: Thirty million dollars for commercial poultry production, $22 million to the dairy industry, $1.6 billion−plus to the timber industry, $90 million for cotton, $19 million for rice, $18 million for soybeans, and $17 million for corn, $17 million for beef cattle, $17 million for catfish, $19 million for the nursery industry, and $5.3 million for the trees/vines sector.
Source: http://deltafarmpress.com/news/060224−hurricane−agriculture/

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

14. *February 24, Journal News (NY)* — **Officials seek laptop with diagram of New York City water system.** New York City police and Department of Environmental Protection (DEP) officials are searching for a stolen laptop computer that includes diagrams of the city water supply system. The laptop contains a diagram of the more than 6,000 miles of New York City water mains, as well as a map of the Jerome Park Reservoir in the Bronx and the Central Park Reservoir in Manhattan. But the laptop does not have details of the upstate reservoir system that includes the New Croton Reservoir, Kensico Reservoir, and other Lower Hudson Valley water supplies, nor is the information considered valuable to would−be terrorists, a DEP official said. So while the DEP is distressed over the missing computer, agency spokesperson Ian Michaels said it is not a great security concern. Michaels said the computer was stolen from a DEP vehicle on Monday, February 20.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20060224/NEWS07/602240351/1023/NEWS07

[Return to top]

Public Health Sector

15. *February 26, Agence France−Presse* — **Almost 90,000 people checked for symptoms of bird flu in India.** Indian officials battling a bird flu outbreak culled hundreds of thousands of chickens and checked around 90,000 people for symptoms in Gujarat state as authorities ordered tests on dead birds at the other end of the country. Ninety−five people suspected of infection tested negative, easing fears the disease might have spread to humans in a country where many live in close proximity with poultry. The government of the northeastern state of Assam sounded a health alert after some 1,000 chickens died, ordering tests on the dead birds. Last week India reported its first cases at Navapur in Maharashtra state south of Gujarat. On

Saturday, February 25, new cases were reported from the neighboring Uchchal area of Surat district in Gujarat, prompting officials to slaughter tens of thousands of chickens.
Source: http://www.todayonline.com/articles/103371.asp

16. *February 26, Interfax* — **Bird flu discovered in six Russian regions.** Bird flu had been registered in six Russian regions as of Sunday, February 26, the Agriculture Ministry's press service said citing the Federal Veterinary and Phytosanitary Control Service. Migrating birds have brought avian flu to the republics of Kabardino−Balkariya, Dagestan, Chechnya and Kalmykia in addition to the Krasnodar and Stavropol territories, the press service said.
Source: http://www.interfax.ru/e/B/finances/26.html?menu=2&id_issue= 11470424

17. *February 25, Agence France−Presse* — **Indonesia records 20th bird flu fatality.** Indonesia's bird flu toll hit the 20 mark with confirmation that a 27−year−old woman had succumbed to the H5N1 virus, the health ministry said. The woman, a housewife who had direct contact with her neighbor's chickens, was admitted to Sulianti Saroso hospital in Jakarta on Monday, February 20, and died the same day, hospital spokesperson Ilham Patu said. Her test results came back from the U.S. on Saturday, February 25, in the middle of an initial three−day crackdown on bird−flu in the Indonesian capital Jakarta that has seen hundreds of birds slaughtered. Some 500 workers and volunteers began a three−day door−to−door sweep on Friday, February 24, in 44 subdistricts of the capital to search for the large number of poultry believed to be living in and around people's homes.
Source: http://news.yahoo.com/s/afp/20060225/hl_afp/healthfluindonesia_060225224612;_ylt=AqHKHRrZKTLSI_bFZkTDyGOJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

18. *February 25, Reuters* — **Cases of crippling fever found in mainland France.** Doctors in mainland France have detected a mosquito−borne disease among people returning from the Indian Ocean region, where the virus is spreading rapidly, a senior health official said on Saturday, February 25. France's health minister has blamed chikungunya for directly or indirectly killing 77 people on the French island of Reunion off the southeast coast of Africa. French health officials say 157,000 people have now been infected by the disease on Reunion, about one in five of the population. The illness has also been found in the Indian Ocean islands of the Seychelles and Mauritius.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://www.alertnet.org/thenews/newsdesk/L25768324.htm

19. *February 25, New York Times* — **Anthrax traces found at three sites as victim worsens.** The Greenwich Village home of a man infected with inhalation anthrax tested positive for the deadly germ, New York City officials said Friday, February 24. Tests on the van and workplace used by the man, Vado Diomande, also tested positive for traces of anthrax. Diomande is the only person found to have been infected with anthrax in this case, which he is thought to have contracted while working with goatskins to make traditional African drums. However, since Thursday, February 23, investigators have expanded their search to include two new locations as they tried to pinpoint the exact origin of the anthrax. The testing done so far supports the hypothesis that the germ was carried on animal skins. Diomande has told investigators that he brought unprocessed skins into the U.S. from Africa. One of the two new locations investigators are looking at is a garage in Brooklyn where they believe Diomande also obtained

animal skins. The police said 50 to 60 animal skins were found stored there and city officials said they were working with Customs officials to determine if they were legally obtained. The other location is a Crown Heights home where a man may have worked with skins obtained from Diomande.
Source: http://www.nytimes.com/2006/02/25/nyregion/25anthrax.html?_r =1&oref=slogin

20. *February 25, Xinhua (China)* — **Two new human cases of bird flu detected in China.** A nine−year−old girl in east China's Zhejiang Province and a 26−year−old woman farmer in east China's Anhui Province were confirmed to be infected with H5N1 bird flu, reported the Ministry of Health on Saturday, February 25. The Zhejiang girl lives in Anji County. She showed symptoms of fever and pneumonia on February 10 and has been hospitalized. According to the investigation, she visited relatives twice in Guangde County of Anhui Province before she fell ill. During her visits, chickens raised at her relatives' homes got sick and some died. The exact source of her infection is under further investigation, said the ministry. The other new case in Anhui is from Yingshang County. She developed fever and pneumonia symptoms on February 11. The patient had contact with sick and dead poultry, according to the investigation. The local agricultural department has isolated H5N1 virus strain from samples of dead chickens in Yingshang County, said the ministry.
Source: http://news.xinhuanet.com/english/2006−02/26/content_4227898 .htm

21. *February 25, Cox News Service* — **Official: Powder found in Texas dorm may not be ricin.** A whitish−brown powder found at the Moore−Hill dormitory on the University of Texas at Austin campus may not be ricin as originally thought, officials said Saturday, February 25. Mike Elliott, senior district commander for Austin−Travis County Emergency Medical Services, said that while one preliminary test returned a positive result for the potentially deadly poison, three subsequent tests done at the Department of State Health Services Lab in Austin were negative. Elliott said the powder placement appears to be random. It was found by a student who was opening a roll of quarters to do laundry. The quarters came from a bank near Houston and were given to the student by her mother at some point last semester. In addition, none of the other people potentially exposed −− including the student with the quarters, her mother, her roommate and their resident hall assistant −− has ricin poisoning symptoms. Elliott also said the powder was heavy and course, not a fine consistency, as a weapon meant to be inhaled would be. As a precaution, weapons of mass destruction experts from Quantico, VA, were in Texas to retrieve and take samples back to federal labs for additional tests, said FBI Special Agent Rene Salinas, a spokesperson with the San Antonio office.
Ricin information: http://www.bt.cdc.gov/agent/ricin/facts.asp
Source: http://www.khou.com/news/state/stories/khou060226_ac_utricin .6648914b.html

22. *February 24, Agence France−Presse* — **H5N1 bird flu found in country of Georgia.** The H5N1 strain of bird flu virus has been found for the first time in the ex−Soviet republic of Georgia, Prime Minister Zurab Nogaideli revealed. Samples have been sent for further testing in London, England. An operation has begun to prevent the further spread of bird flu in the Adjara region under the direction of President Mikheil Saakashvili. Preventive work is also being carried out in areas bordering Azerbaijan and Turkey. The discovery of the virus in Georgia follows outbreaks in neighboring Azerbaijan, Iran, Turkey, and Russia.
Source: http://news.yahoo.com/s/afp/20060224/hl_afp/healthflugeorgia _060224124429;_ylt=AtBb2WgULAarYjY.K_kHjNqJOrgF;_ylu=X3oDMTA

5aHJvMDdwBHNlYwN5bmNhdA−−

23. *February 24, Reuters* — **South Korea says humans infected with bird flu 2003−04.** Four South Koreans were infected with the H5N1 strain of bird flu in late 2003 and early 2004 but none of them developed any serious illnesses, a South Korean health official said on Friday, February 24. These four are the first people in the country confirmed to have been infected with the H5N1 strain, Oh Dae−kyu, the head of the Korea Center for Disease Control and Prevention said. South Korea becomes the eighth country to report a human infection of the H5N1 strain since 2003. About 400,000 poultry at South Korean farms were infected by bird flu between December 2003 and March 2004, but no human cases were reported at that time. That outbreak marked bird flu's re−emergence and was followed by cases around the world involving the H5N1 strain. The ministry had sent blood samples of 318 poultry industry workers to the U.S. Centers for Disease Control and Prevention for tests and received confirmation of the antibodies in the blood of the four on Thursday, February 23.
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006−02−24T134844Z_01_SEO224633_RTRUKOC_0_US−BIRDFLU−KOREA.xml&archived=False

24. *February 23, Reuters* — **West Nile virus still a threat.** The West Nile virus remains a serious health risk in the U.S. even though the number of cases has plunged, a U.S. health official said on Thursday, February 23. "We are entering a new phase, and we can call it the endemic phase," said Lyle Petersen, director of the U.S. Centers for Disease Control and Prevention's Division of Vector−Borne Infectious Disease. "The virus is here and it's going to stay," Petersen told reporters at the National Conference on West Nile Virus in the U.S. Last year 2,949 human cases of West Nile were reported in the U.S. Of those infected, 116 died. Those figures are down dramatically from 2003, when the virus peaked at some 10,000 cases and 264 fatalities. Petersen said the drop in cases may lead to complacency, noting the virus over the past three years was the most common infection transmitted by mosquitoes in North America.
West Nile information: http://www.cdc.gov/ncidod/dvbid/westnile/index.htm
Source: http://today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006−02−23T225544Z_01_N23534860_RTRUKOC_0_US−WESTNILE.xml&archived=False

[Return to top]

Government Sector

25. *February 25, Del Rio News Herald (TX)* — **Package threat closes Texas police department, courthouses.** A suspicious package shut down operations at the Del Rio Police Department station for about six hours Thursday afternoon, February 23, and caused evacuations of the downtown post office building, two courthouses and several businesses. “Because of information we had on the package, we felt we had strong enough cause to take this to the next level, to take it seriously,” said Del Rio Fire & Rescue Department Deputy Chief John Sheedy. He said a bomb disposal unit from Lackland Air Force Base in San Antonio was requested. The federal courthouse and the businesses in the 200 and 300 blocks of South Main Street were ordered evacuated. The police and fire departments also evacuated the police station, the East Broadway Post Office, and the Val Verde County Judicial Center. The Lackland bomb disposal

team used an F6A wheeled robot to pick up the suspicious package and carry it into the vacant parking lot on the north side of the post office building. Then the robot used a type of water cannon to destroy the package. An investigation regarding the incident is ongoing.
Source: http://www.delrionewsherald.com/story.lasso?ewcd=6341d2afd46 e1b9e

[Return to top]

Emergency Services Sector

26. *February 24, New York Times* — **Albany's plan for flu epidemic leaves big decisions to localities.** Each county in New York would be responsible for formulating its own response plan in the event of an outbreak of pandemic influenza in the state, according to the formal preparedness plan made public Thursday, February 23, by the state's Department of Health. While state health workers would offer guidance and help coordinate the response, the plan calls for critical decisions −− like establishing quarantine measures and deciding whether to close schools and businesses −− to be decided largely on a local level. Almost immediately, the plan drew criticism from outside experts who contend that simply providing a template for localities without adequate resources in the form of equipment, money and expertise could prove disastrous. At 400 pages, the state plan focuses on three main areas: early detection, prevention, and delivery of care. Dr. Antonia Novello, the state health commissioner, acknowledged that the plan was evolving, and she said the goal was essentially to give the localities a framework so they could create their own plans. State officials, however, could not provide specific details on matters as basic as how many additional ventilators the state has or how much antiviral medication has been stockpiled.
Source: http://www.nytimes.com/2006/02/24/nyregion/24flu.html?_r=1&o ref=slogin

27. *February 23, Homeland Response (OH)* — **Tennessee district obtains new emergency notification system.** Through Department of Homeland Security funds, Tennessee Homeland Security District 7 officials have acquired a new Telephone Emergency Notification System which will be used before, during and after emergency situations, such as terrorist threats or flooding evacuations. The technology is an Internet−based calling engine. It will allow the district to rapidly alert residents in their homes and mobilize first responders, including police, fire, EMS, and emergency management.
Source: http://www.homelandresponse.org/500/BreakingNews/Article/False/13431/BreakingNews

28. *February 22, Connection Newspapers (VA)* — **Northern Virginia conducts simulation to assess emergency preparedness.** Herndon, VA, officials recently simulated a four−hour emergency preparation exercise. Called the "Patriot Challenge II," Herndon was one of 11 localities in the Northern Virginia area that participated in the computer simulation. The challenge was designed to enact and assess emergency preparedness systems in localities throughout the region. Through the exercise, Herndon staff coordinated responses with other participants throughout the region including Federal Bureau of Investigation agents, Fairfax County Police Officers and other department heads, Mayor Michael O'Reilly said. O'Reilly was on hand to watch the simulation as well as act the part of the seven−member Town Council. "We were able to see who would declare a state of emergency, and what that means procedurally," O'Reilly said. The simulation also gave the town a chance to see how its

inter−departments would communicate not only with each other during a disaster, but also with other jurisdictions in the area. Stationed in the Herndon Police Department community room, town staff used computers via WebEOC, a portal that facilitates multi−jurisdictional and multi−agency communications and coordination in the event of an emergency. By using this program, participants could easily communicate with each other what they were doing in their respective areas.
Source: http://www.connectionnewspapers.com/article.asp?article=6231 1&paper=66&cat=104

[Return to top]

Information Technology and Telecommunications Sector

29. *February 23, SC Magazine* — **Feebs variant threatening users.** There is a new version of the W32/Feebs worm in the wild, which contains a ZIP attachment and claims to be a secure e−mail message, contains exploit code that triggers a download from a number of malicious sites, the SANS Institute's Internet Storm Center said Wednesday, February 22. The SANS Institute said the newest version of the worm claims to be from a Gmail user.
Source: http://www.scmagazine.com/uk/news/article/543251/feebs−varia nt−threatening−users/

30. *February 23, FrSIRT* — **Macromedia Shockwave Player installer buffer overflow vulnerability.** A vulnerability has been identified in Macromedia Shockwave Player, which could be exploited by remote attackers to take complete control of an affected system. Analysis: This issue is due to a stack overflow error in the ActiveX installer that does not properly handle overly large values passed to certain parameters, which could be exploited by attackers to execute arbitrary commands by tricking a user into visiting a malicious Website with Shockwave content that prompts the user to install the player. Affected products: Macromedia Shockwave Player version 10.1.0.11 and prior.
Solution: The vendor has fixed the issue in the Shockwave Player ActiveX installer.
Note: Since the vulnerability occurs in the installer, no action needs to be taken by users.
Source: http://www.frsirt.com/english/advisories/2006/0716

31. *February 23, Security Focus* — **Nullsoft Winamp M3U file processing buffer overflow vulnerability.** Winamp is a popular media player that supports various media formats and playlist formats, including m3u and pls formats. Analysis: Winamp can play files by loading .m3u file. When the playing is paused or stopped, Winamp will reset the title of the program, where function strncpy() is incorrectly called, resulting in a static buffer overflow. An attacker can cause winamp to crash by crafting a malicious .m3u file Vulnerable products: Vulnerable: NullSoft Winamp 5.13 and NullSoft Winamp 5.12.
Solution: This issue has been addressed in Winamp 5.2:
NullSoft Winamp 5.12: NullSoft Winamp 5.2: http://www.winamp.com/player/
NullSoft Winamp 5.13: NullSoft Winamp 5.2: http://www.winamp.com/player/
Source: http://www.securityfocus.com/bid/16785/references

32. *February 23, Tech Web* — **Zero−day exploit turns up heat on Mac OS X.** An exploit for the recently−disclosed zero−day vulnerability in Apple Computer's Mac OS X has gone public, security vendors said Thursday, February 23, increasing the risk that the bug will be used by

attackers. Code has been posted to the Metasploit Project site. The code targets the so−called "Safe file" flaw in Apple's Safari browser.
Source: http://www.techweb.com/wire/security/180206995;jsessionid=HZO4DQY1MGY2GQSNDBOCKHSCJUMEKJVN

33. *February 23, Tech Web* — **Report: Homeland Security to get big IT spending boost.** The Department of Homeland Security (DHS) is expected to get the lion's share of new IT technology spending, according to an analysis of an Office of Management and Budget study that was released Thursday, February 23. The DHS increase of some $772 million represents 44 percent of new federal IT outlays, reported government market research firm Input. Overall, in fiscal year 2007, federal agencies are planning to spend a total of $64.3 billion on IT.
Source: http://www.techweb.com/wire/ebiz/180206942;jsessionid=HZO4DQY1MGY2GQSNDBOCKHSCJUMEKJVN

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:

VU#999708 − Apple Safari may automatically execute arbitrary shell commands

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser document.

Public Exploit Code for Buffer Overflow Vulnerability in Microsoft Windows Media Player Plug−in for Non−IE Browsers

US−CERT is aware of publicly available exploit code for a buffer overflow vulnerability in Windows Media Player plug−in for browsers other than Internet Explorer (IE). For more information can be found in the following US−CERT Vulnerability Note:

VU#692060 − Microsoft Windows Media Player plug−in buffer overflow
http://www.kb.cert.org/vuls/id/692060

US−CERT urges users to apply appropriate updates and review the workarounds listed in the Microsoft Security Bulletin MS06−006 to mitigate this vulnerability.
http://www.microsoft.com/technet/security/Bulletin/MS06−006. mspx

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 2234 (directplay), 5435 (dttl), 139 (netbios−ssn), 32774 (sometimes−rpc11), 135 (epmap), 4133 (nuts_bootp) 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

34. *February 25, Associated Press* — **Smart cameras, guards to protect World Trade Center site.** Visitors to the complex that eventually will fill the World Trade Center site might have to submit to iris scans or thumb print analysis to get into buildings, while smart cameras try to match their faces to a photo database of known terrorists. Well−paid armed guards would be on patrol and sensors would test the air for lethal gases. Preliminary details of a plan to make the redeveloped 16−acre site as terrorism−proof as possible were provided to The Associated Press this past week by former FBI agent James Kallstrom, Governor George Pataki's senior counterterrorism adviser. Kallstrom and city and federal officials are aiming for a higher standard of security than is currently in use for public spaces around the nation. The Port Authority of New York and New Jersey, which owns the site and has its own police force, could share responsibility for the site with city police and highly trained, armed security guards.
Source: http://news.yahoo.com/s/ap/20060225/ap_on_re_us/ground_zero_security;_ylt=Au7uBsPzDV9L5tuIYoWFRMhG2ocA;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[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.