Department of Homeland Security Daily Open Source Infrastructure Report for 31 January 2006

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

Daily Highlights

- Federal Computer Week reports Russian hackers broke into a Rhode Island government Website and stole credit card data from individuals who have done business online with state agencies. (See item 8)
- Department of Homeland Security Secretary Michael Chertoff has announced the further implementation of Expedited Removal to include the entire U.S.−Canadian border and all U.S. coastal areas, as part of the Secure Border Initiative. (See item 18)
- The Associated Press reports the Giant supermarket chain has pulled soup cans from its stores in four states after a Pennsylvania family reported finding a sewing needle in a sealed can of minestrone; this was the fourth report of needles or pins found in food purchased from area stores in the past two weeks. (See item 22)

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 30, Agence France−Presse* — **Russia to mine rare fuel on moon.** Russia is planning to mine a rare fuel on the moon by 2020 with a permanent base and a heavy−cargo transport link. According to Nikolai Sevastyanov, head of the Energia space corporation: "We are

planning to build a permanent base on the moon by 2015, and by 2020, we can begin the industrial−scale delivery...of the rare isotope helium−3." The International Space Station would play a key role in the project, and a regular transport relay to the moon would be established, Sevastyanov said. Helium−3 is a non−radioactive isotope of helium that can be used in nuclear fusion. Rare on earth but plentiful on the moon, it is seen by some experts as an ideal fuel because it is powerful, nonpolluting, and generates almost no radioactive byproduct.
Source: http://www.washingtontimes.com/world/20060129−113631−6996r.h tm

2. *January 29, Associated Press* — **Dirty bomb sensors are tested at Nevada site.** Homeland security scientists are conducting a Radiological−Nuclear Countermeasures Test and Evaluation Complex in the Nevada desert, 75 miles north of Las Vegas. The $33 million program is designed to perfect devices that can more accurately detect nuclear devices and "dirty bombs." The program, a division of the Department of Homeland Security, was created under a presidential order to refine methods to protect the nation from radiological and nuclear threats. The test site also is home to the National Center for Combating Terrorism, which includes several facilities to improve the nation's ability to prevent or recover from a terrorist attack. Technicians are testing sensors that detect neutrons and gamma rays emitted by lethal nuclear devices or radioactive isotopes that could be dispersed by less sophisticated explosives in a dirty bomb. The tests aim to determine whether the 30 or so devices available commercially can distinguish a bomb from less harmful sources of radioactivity, such as a person who has had a radioactive isotope injected during a medical procedure, or household items like kitty litter and floor tiles that contain natural trace amounts. Of the 10,000 alarms tallied to date across the nation, all have been resolved by closer inspections.
Source: http://www.buffalonews.com/editorial/20060129/1023825.asp

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *January 30, Chicago Tribune* — **Worker dies in explosion of tank at asphalt plant.** An explosion at a Chicago asphalt company Sunday, January 29, killed one worker. The explosion occurred just after 1 p.m. CST Sunday at Gardner Asphalt Corp., 4718 W. Roosevelt Rd., where one of four outdoor tanks caught fire, said Kevin MacGregor of the Fire Department. The nearly 30−foot−tall tank most likely contained asphalt, which ignited for an unknown reason, MacGregor said, adding that firefighters prevented the other tanks from catching fire. "We will be doing an investigation for cause and the origin of the fire," he said.
Source: http://www.chicagotribune.com/news/local/chicago/chi−0601300122jan30,1,2070615.story?coll=chi−newslocalchicago−hed

4. *January 30, Journal News (NY)* — **Cause found for tanker spill in New York.** Cleanup continued for a third day Monday, January 30, after a gasoline spill on a New York Interstate−95 ramp Saturday, January 28, and police say they found the cause of the accident. State police determined that the mechanical failure of the so−called fifth wheel −− the pivot point between the tractor and its trailer −− caused the tanker to roll over at Exit 15 in New Rochelle, NY. The accident spilled 2,000 gallons of gasoline on the road, closing the northbound entrance and exit ramps for 12 hours Saturday. The accident also forced the precautionary closing of a nearby Costco and a two−hour suspension of Amtrak service along

the Northeast Corridor, whose train tracks run alongside I−95. No one was injured, but 2,000 of the 8,000 gallons of Getty fuel carried by the tanker truck spilled onto the roadway. An undetermined amount entered storm drains and the Burling Brook stream, which runs through the Pelham Country Club golf course and empties into the Sound near Glen Island Park.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20060130/NEWS02/601300353/1025/NEWS09

5. *January 28, Greeley Tribune (CO)* — **Chemical spill prompts evacuations in Colorado.** A chemical smell settled in Greeley, CO, Friday afternoon, January 27, sending 16 people to the hospital and caused about 200 people to be evacuated from the TriPointe Business Center in Evans for an hour. Mercaptan, the smelly chemical added to odorless natural gas that alerts people to leaks, spilled at the site of Miller's Greenhouse and Renewable Fiber in Greeley. Evans Fire Department got its first report of the smell at 1:50 p.m. MST, said Captain Robert Standen. One person was admitted at the North Colorado Medical Center in Greeley Friday afternoon and later released, according to hospital officials. All others were treated and released. A gas well on the Miller's Greenhouse property was capped for two to three years and an owner was moving a storage container with mercaptan, said Atmos Energy spokesperson Karen Wilkes. Although Atmos was not responsible because it does not own the mercaptan that was spilled, representatives still responded to check gas lines in the area, Wilkes said.
Source: http://www.greeleytrib.com/article/20060128/NEWS/101280079

[Return to top]

Defense Industrial Base Sector

6. *January 30, Aviation Week* — **Boeing restructuring its defense business.** Moving to improve profit margins and position itself for an anticipated slowdown in Pentagon spending in fiscal 2007, Boeing on Friday, January 27, unveiled a major restructuring of its defense business. Boeing Integrated Defense Systems (IDS), which has annual sales of more than $30 billion, is being consolidated from seven units to three: Precision Engagement and Mobility Systems, Networks and Space Systems, and Support Systems. The Department of Defense's second−largest contractor also is making IDS responsible for overseeing some technology development programs at its Phantom Works enterprise. Jim Albaugh, president and CEO of IDS, told reporters the reorganization was aimed at improving productivity and execution while positioning the company for a new era of leaner U.S. defense spending. The consolidation will likely cause "a few" layoffs, but no closures of major IDS facilities are planned, Albaugh said. IDS was a major bulwark for Boeing during the commercial aircraft downturn earlier in the decade, providing 58 percent of the company's revenue in 2004. And while IDS continues to post double−digit profit margins, anticipated cuts to Pentagon programs have sent defense contractors scrambling to find new ways to generate revenue growth.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/BOER01306.xml

[Return to top]

Banking and Finance Sector

7. *January 30, Finextra* — **Fraud in UK at highest level in ten years.** Large value fraud in the UK rocketed in 2005, with a surge in the second half of the year resulting in fraud up nearly three times from the previous year, and the highest recorded level since 1995, according to KPMG Forensic's Fraud Barometer. The research saw 222 cases reaching court over the course of 2005, up from 174 cases in 2004. The past six months have seen an explosion of fraud case prosecutions, many of them high value. A little under half of fraud was carried out by professional gangs, but even more was the result of 'insider' fraud by management or company employees. Jeremy Outen, partner at KPMG Forensic, says the number and the average value of frauds is increasing. Recent cases against financial institutions include instances of an employee feeding information or sending funds to outside accomplices. Employees placed or groomed by criminal gangs has been flagged in recent months by the Financial Services Authority. Identity fraud continues to be rife, as scammers seek ways around the tighter controls introduced by such measures as chip and PIN. Phishing scams on the Internet are a common way of obtaining people's identities and bank details and continue to proliferate.
Source: http://finextra.com/fullstory.asp?id=14829

8. *January 27, Federal Computer Week* — **Hackers steal credit card info from Rhode Island Website.** Russian hackers broke into a Rhode Island government Website and allegedly stole credit card data from individuals who have done business online with state agencies. The Providence Journal reports that the hackers boasted two weeks ago on a Russian−language Website that they broke into the government Website and stole credit card information for as many as 53,000 transactions. State officials said the Website was breached Wednesday, December 28, 2005. The site is managed by New England Interactive, which that manages 17 other state portals. Renee Loring, a spokesperson for the Website, confirmed that a server database was breached and encrypted credit card information was obtained. The company is working with law enforcement officials to resolve the matter. Internal and external security audits were conducted with a third−party provider since the incident. The Russian Website displayed images of how the hackers were breaking into the state portal. According to the newspaper, the final image shows “a list of 38 credit card accounts the hackers claim to have stolen...Part of the screen is blocked by a black rectangle emblazoned ‘CENSORED’ in white letters in English. The rectangle covers part of the credit card number, but some digits are not hidden.”
Website: http://www.RI.gov
Source: http://www.fcw.com/article92132−01−27−06−Web

9. *January 27, The Register (UK)* — **Police arrest AOL phishing suspect.** A California man who allegedly duped AOL users into handing over credit card details to a fraudulent website has been arrested in the U.S. Police charged Jeffrey Brett Goodin, 46, of Azusa, with wire fraud and other charges over allegations he masterminded an aggressive phishing scam. Goodin allegedly sent thousands of emails that posed as messages from AOL's billing department warning customers needed to update their payment information or risk losing access to their accounts. Customers were directed towards a fraudulent website and invited to hand over sensitive personal details including credit and debit card information that Goodin allegedly used to make fraudulent purchases.
Source: http://www.theregister.com/2006/01/27/aol_phishing_suspect_a rrest/

10. *January 27, The Register (UK)* — **ChoicePoint fined $15 million over data security breach.** On Thursday, January 26, data broker ChoicePoint was fined $15 million over a data security breach that led to at least 800 cases of identity theft. It also agreed to maintain a revamped security program, featuring regular third−party security audits until 2026, and promised to ensure it provides consumer reports only to legitimate businesses. Scammers obtained credit reports, social security numbers, and other sensitive information of more than 163,000 consumers on ChoicePoint's database after scammers successfully made bogus applications to establish more than 50 accounts with the credit reference firm. ChoicePoint is a credit reference agency whose clients include the U.S. Government and credit card firms. The Federal Trade Commission (FTC) alleges that ChoicePoint failed to screen prospective subscribers and turned over consumers' sensitive personal information to obviously dubious subscribers. ChoicePoint approved the applications of individuals who lied about their credentials. The FTC charged that ChoicePoint violated the Fair Credit Reporting Act by furnishing consumer credit histories to subscribers without properly checking their identity. FTC chairman Deborah Platt Majoras said, "Data security is critical to consumers, and protecting it is a priority for the FTC, as it should be to every business in America."
    Source: http://www.theregister.com/2006/01/27/choicepoint_ftc_settle ment/

11. *January 27, Networkworld* — **Thief steals backup data on 365,000 patients.** About 365,000 hospice and home health care patients in Oregon and Washington are being notified about the theft of computer backup data disks and tapes last month that included personal information and confidential medical records. On Thursday, January 26, Providence Home Services said the records and other data were on several disks and tapes stolen from the car of a Providence employee. The incident was reported by the employee on Saturday, December 31. The tapes and disks were taken home by the employee as part of a backup protocol that sent them off−site to protect them against loss from fires or other disasters. That practice has since been stopped, said health system spokesperson Gary Walker. "This was only done in one area of the company," Walker said. Some of the data was stored in proprietary file formats without password−protection. From now on, all data will be made secure using additional technologies, according to Walker. Providence officials said there have been no reports that any of the stolen information has been used improperly since the incident. The information on the disks and tapes included names, addresses, dates of birth, physicians' names, insurance data, social security information, and financial information.
    Source: http://www.networkworld.com/news/2006/012706−patients.html

[Return to top]

Transportation and Border Security Sector

12. *January 30, Register (UK)* — **Face and fingerprints swiped in Dutch biometric passport crack.** Dutch TV program Newslight is claiming that the security of the Dutch biometric passport has already been cracked. As the program reports, the passport was read remotely and then the security cracked using flaws built into the system, at which point all of the biometric data could be read. The crack is attributed to smartcard security specialist Riscure, which explains that an attack can be executed and the security broken, revealing date of birth, facial image, and fingerprint, in around two hours. Riscure notes that the speed of the crack is aided by the Dutch passport numbering scheme being sequential. Bart Jacobs, Research Director of

the Institute for Computing and Information Sciences, University of Nijmegen, says that a skimming exercise could potentially yield all biometric data from a passport (or a biometric ID card), giving ID thieves and would−be forgers a considerable leg up in the construction of fakes.
Source: http://www.theregister.com/2006/01/30/dutch_biometric_passpo rt_crack/

13. *January 30, Union−Tribune (CA)* — **Smuggling tunnel details.** Last week, agents with U.S. Immigration and Customs Enforcement discovered the passageway that was the exit point for drug smugglers who built a massive underground tunnel to bring tons of marijuana into the United States from Tijuana. It runs 2,400 feet, or the length of about eight football fields, and is equipped with lighting, ventilation and groundwater drainage. From the outside, the site is unremarkable. The tunnel starts in the floor of a plain white office attached to a large warehouse in Otay Mesa. The nine−square−foot tunnel door is on wheels so smugglers could roll it across the floor on their way up. A hole about eight feet deep gapes beneath the door. At the bottom is a kitchen stool smugglers used to boost themselves into the office. Parts of the shaft are about 70 feet deep. The walls are sandstone and compacted sand, but look more like a mix of rock and dark clay. Wood supports were used, but only sporadically because the earth is extremely dense. Agents believe the tunnel, one of the largest and most sophisticated ever found along the California−Mexico border, is the work of a drug cartel.
Source: http://www.signonsandiego.com/news/mexico/tijuana/20060130−9 999−1m30secret.html

14. *January 30, Associated Press* — **Washington track repaired and reopened.** There were no serious injuries when the Chicago−bound Amtrak passenger train derailed early Saturday, January 28, about 45 miles west of Spokane, WA. Burlington Northern Santa Fe crews had the locomotive and four cars rerailed by nightfall, and then worked through the night to repair the track, spokesperson Gus Melonas said. The derailed train was covering the Empire Builder route between Chicago and Portland, OR, which offers one eastbound and one westbound train daily. Passengers from the derailed train were bused to Spokane hotels before dawn Saturday, and took the Saturday night train to the Midwest. The cause of the derailment is under investigation, Melonas said.
Source: http://seattlepi.nwsource.com/local/6420AP_WA_Train_Derailed .html?source=mypi

15. *January 30, Associated Press* — **Airports begin new security rules.** Tens of thousands of employees at airport restaurants, newsstands and other shops behind security checkpoints will soon have to undergo more detailed background checks and pass through metal detectors on their way to work. New directives issued late Tuesday, January 24, by the Transportation Security Administration (TSA) also require all 445 commercial airports to reduce the number of doors behind security checkpoints used by airport and airline employees, and increase security for the remaining doors. TSA spokesperson Mark Hatfield Jr. said Wednesday, January 25, the new rules are designed to strengthen security and "identify and disrupt potential threats to civil aviation." Under the new rules, private employees will pass through screening every day on their way to work. In addition, the TSA will require airports to reduce the number of security identification badges issued to vendor employees. Such badges allow access beyond the secure area to airport tarmacs and the airplanes themselves. Passengers and airline employees are already required to pass through screening areas before being allowed to enter gate areas. The TSA, looking to speed that process, began a pilot program in Minneapolis on Wednesday that

allows frequent fliers to avoid random searches by submitting to background checks in advance.
Source: http://www.wcnc.com/sharedcontent/nationworld/washingtonprint/070704cckttwWashTSARules.2d69975c0.html

16. *January 30, CNN* — **In−flight phones not wanted.** A new survey has found that the majority of business travelers are opposed to allowing cell phone use on board aircraft. Until now, most airlines have outlawed phone use, claiming possible interference with aircraft electronics. The ban also prevents onboard cell phones disrupting communications on the ground as they sweep through regionalized networks at high speed. But all this is set to change in December 2006, following revisions by U.S. federal regulators. At that time, flights will able to carry an onboard transmitter that will link the aircraft to satellites, allowing passengers to use their mobile phones as normal. But, according to a survey by Carlson Wagonlit Travel, which quizzed 2,100 business travelers and 650 travel managers, most are unlikely to welcome the phones.
Survey: http://www.carlsonwagonlit.com/export/sites/cwt/en/countries/us/media_relations/news/CWT_Indicator_regional_results_01.2 3.06.pdf
Source: http://www.cnn.com/2006/TRAVEL/01/30/plane.phone/

17. *January 30, Bellingham Herald (WA)* — **One−day border passcard debated.** Federal officials may create a one−day pass to allow people to cross the border without a passport or special identification card, according to a report on a Senate hearing Wednesday, January 25. Such a pass could allow people to cross the border "for one day on a little whim," US−VISIT Program Director Jim Williams told the Senate's Appropriations Subcommittee on Homeland Security, according to Congressional Quarterly. A 2004 law calls for requiring everyone entering the United States to present a passport or other secure identity and citizenship documentation. Officials plan to require this for all air and sea travel from Canada and Mexico beginning December 31 and for all land travel at the end of 2007. The "People Access Security Service" card would cost less than a passport but would be only for Americans and would still be too expensive and take too long to get, according to critics. U.S. Senator Patty Murray (D−WA), pushed at the hearing for delaying passport requirements for sea and air crossings. "Washington state has a robust tourism industry that has historically depended on fluid cross−border travel," Murray said.
Source: http://www.bellinghamherald.com/apps/pbcs.dll/article?AID=/20060130/NEWS03/601300346

18. *January 30, Department of Homeland Security* — **DHS streamlines removal process along entire U.S. border.** Department of Homeland Security (DHS) Secretary Michael Chertoff announced on Monday, January 30, the implementation of Expedited Removal (ER) along the entire U.S.−Canadian border and all U.S. coastal areas, as part of the Secure Border Initiative. This announcement reflects the further implementation of ER that was initially implemented along the Southwest border and will now be implemented along all of the United States' border areas. ER is an effective border management process that swiftly returns illegal aliens to their countries of origin while maintaining protections for those who fear persecution. ER provides DHS the authority to expeditiously return applicable illegal aliens to their country of origin as soon as circumstances will allow. DHS will be applying ER to aliens who have spent 14 days or less in the United States, and are either apprehended within 100 miles of the border with Mexico or Canada or arrive by sea and are apprehended within 100 miles of a coastal border

area. ER disrupts the various human smuggling cycles that occur along the border by substantially reducing the time from arrest to ultimate removal from the United States and foreclosing opportunities for these illegal aliens to reconnect with their smugglers and guides. Customs and Border Patrol Overview: http://www.cbp.gov/xp/cgov/border_security/border_patrol/ove rview.xml
Source: http://www.dhs.gov/dhspublic/display?content=5377

[Return to top]

Postal and Shipping Sector

19. *January 30, Logistics Management (MA)* — **FedEx to boost presence in China.** The global shipping giant FedEx has signed an agreement to acquire Tianjin Datian W Group's (DTW Group) 50 percent share of the FedEx−DTW International Priority express joint venture and DTW Group's domestic express network in China. The acquisition will include DTW Group's 50 percent share in the International Priority express joint venture, converting the joint venture into a wholly FedEx−owned company. Upon closure of the deal, FedEx will employ more than 6,000 people in China.
Source: http://www.logisticsmgmt.com/index.asp?layout=articleXml&xml Id=348953714

[Return to top]

Agriculture Sector

20. *January 30, Purdue University Exponent* — **Game show helps workshop attendees understand problems with crops.** Friday, January 27, attendees at one of Purdue University's Crop Management Workshops had the opportunity to play Pestardy! −− a game that tested contestants' knowledge of crop maladies. The Crop Management Workshops are designed to help farmers and agribusiness people learn how to protect their crops from pests. Five workshops were held throughout Indiana from January 23 to 27. In the game, all clues were visual. Contestants buzzed in if they recognized the pest, weed, or plant disease symptom pictured on a screen. Corey Gerber, director of Purdue's crop diagnostic training and research center, said he had hosted five games in the past week. One at each of the agricultural workshops held throughout the state. Gerber said 2006 was the first year the game was played. "We came up with the idea to help train people in the agriculture community. We thought the game would be entertaining but also educational," he said.
Source: http://www.purdueexponent.org/index.php/module/Issue/action/ Article/article_id/2602

21. *January 30, Agence France−Presse* — **Foot−and−mouth disease detected in Russia.** An outbreak of foot−and−mouth disease (FMD) has been detected in eastern Russia, close to the border with China. Hundreds of cows and dozens of pigs in the village of Srednaya Borza, in Chita region, were showing symptoms of the disease, ITAR−TASS news agency quoted emergency situations ministry officials as saying on Monday, January 30. The area was affected by FMD in 2005.
FMD information: http://www.aphis.usda.gov/lpa/pubs/fsheet_faq_notice/fs_ahfm d.html
Source: http://www.breitbart.com/news/2006/01/30/060130174457.g39pt6 o2.html

[Return to top]

Food Sector

22. *January 30, Associated Press* — **Supermarket pulls soup after needle found.** A supermarket chain pulled soup cans from the shelves of its stores in four states after a Pennsylvania family reported finding a sewing needle in a sealed can of minestrone, officials said. The incident was the fourth report of needles or pins found in food purchased from area stores in the past two weeks. The soup was purchased Saturday, January 28, at a Giant Food Store in Wind Gap, PA. Company spokesperson Dennis Hopkins said store personnel pulled cans with similar lot numbers from shelves of all stores as a precaution. He said the chain was also increasing its undercover security until further notice. Giant, owned by the Dutch food company Ahold Ltd., operates 122 supermarkets in Pennsylvania, Maryland, Virginia, and West Virginia. Last week, at another Giant store near Bethlehem, PA, a man reported finding a rusty sewing needle in a loaf of bread. Other incidents were at a King's Supermarket in Bethlehem, in which customers and employees reported finding pins in an onion, packages of ground beef, and a ham.
Source: http://abcnews.go.com/US/wireStory?id=1556855

23. *January 30, Daily Bulletin (CA)* — **Authorities seize "bathtub" cheese.** Authorities seized 600 pounds of "bathtub" cheese from a small ranch in southwest Riverside, CA. The seizure of the illegally produced cheese was one of the largest on record in the state, according to the California Department of Food and Agriculture (CDFA). The cheese was seized Saturday, January 28, by a multiagency task force that included CDFA officers, Ontario police and Riverside and San Bernardino County sheriff's deputies. Two men at the ranch were cited for illegal cheese production. Officials refer to illegally produced cheese as "bathtub" cheese because of the often unsanitary conditions in which it is made. Dirty production techniques encourage the growth of harmful bacteria such as salmonella and listeria, which pose serious health risks, according the CDFA. CDFA spokesperson Steve Lyle said he didn't know where this cheese was being sold. But illegally produced cheese is most commonly sold on the streets and at open−air markets.
Source: http://www.dailybulletin.com/news/ci_3445671

24. *January 29, Austin American Statesman (TX)* — **Key concern for grocers will be fresh shipments.** Grocers should expect a spike in demand during a pandemic, said Tim Hammonds, president of the Food Marketing Institute, which represents food retailers and wholesalers. The institute hasn't devised a plan for a pandemic, Hammonds said, but he expects a health care emergency plan to be incorporated into the industry's overall disaster preparation. Stores would have time to stockpile key supplies, including water, face masks, canned goods, frozen foods, batteries, vitamins, cold remedies and other items, Hammonds said. But fresh food supplies might be tight, he said. In general, stores get several deliveries a week, but if many truckers were out sick, he said, regions not being hit by the pandemic could help those under siege. "There is a lot of excess capacity and flexibility built in there," he said. Pharmacy chains can reroute supplies immediately when demand increases, said Karen Reagan, vice president of the Texas Retailers Association, which represents groceries and pharmacies. Food, water and fuel shipments would be top priorities, said Bill Webb, president of the Texas Motor Transportation Association. Given the fragmented nature of the trucking industry, with 40,000 companies and

300,000 commercial drivers, "it would be difficult" to come up with a comprehensive and binding emergency plan, he said.
Source: http://www.statesman.com/news/content/news/stories/local/01/ 29pandemicfood.html

25. *January 27, U.S. Food and Drug Administration* — **Teethers recalled.** The First Years, a subsidiary of RC2 Corporation, is voluntarily recalling liquid filled teethers due to possible bacterial contamination. The liquid inside the teethers may contain pseudomonas aeruginosa and pseudomonas putida which can cause serious illness in children if the teether is punctured and the liquid from the teether is ingested. This recall is for six different styles of liquid−filled teethers for infants (three plus months old) to soothe gums during the feeding stage. No illnesses have been reported to date in connection with this problem. The teethers are sold nationwide including major retailers, grocery, drug and specialty stores.
Source: http://www.fda.gov/oc/po/firmrecalls/firstyears01_06.html

[Return to top]

Water Sector

26. *January 29, Associated Press* — **City to use water fleas in security measure.** Much as coal miners used canaries to detect toxic gases in mines, Altoona, PA, will use a type of water flea to test reservoirs for toxins that could be dumped by terrorists. The Altoona City Authority's current testing looks for mostly organic compounds that can leach into its 13 reservoirs, but does not check for poisons. Use of the tiny crustaceans, which are hypersensitive to poisons, will take care of that. To test the water, examiners add sugar that is tagged with a fluorescent marker that does not glow while connected to the sugar. In unpoisoned water, the fleas digest the sugar and break the marker away, and the glow can then be seen within the translucent bodies of the animals. In poisoned water, however, the fleas grow sick, can't digest the sugar and will not glow. Officials say the system is not foolproof, since normal substances in the water can interfere with the results. Altoona plans to test its water weekly and will also conduct emergency tests.
Source: http://www.philly.com/mld/philly/news/13743530.htm

27. *January 27, Miami Herald (FL)* — **Miami−Dade's long−term water plans could hamper future growth, officials warn.** Florida state water managers warned Miami−Dade County on Thursday, January 26, to come up with a new plan for supplying water to its booming population over the next two decades −− one that doesn't blatantly ignore state conservation requirements. Miami−Dade, they said, doesn't have more water to give, at least not from the cheap source the county's utility currently taps. The stern warning does not mean there won't be enough water for current residents. But it does have profound implications for the coming years, from hiking water rates to derailing new development −− including a push to build thousands of new homes, shops, and offices on the fringes of the Everglades. Under new growth management laws the state Legislature passed last year, counties are supposed to show they have the water to supply the demands of new development. Revamping the county's water supply will likely require millions of dollars in new infrastructure and technology.
Source: http://www.miami.com/mld/miamiherald/13722835.htm

[Return to top]

Public Health Sector

28. *January 30, Associated Press* — **Officials confirm bird flu death of Iraqi.** Iraqi and United Nations health officials said Monday, January 30, a 15−year−old girl who died this month was a victim of the H5N1 strain of the bird flu virus, the first confirmed case of the disease in the Middle East. Tests were under way to determine if the girl's 50−year−old uncle, who lived in the same house, also died of the virus. Shangen Abdul Qader died January 17, just 10 days before her uncle, Hamasour Mustapha, who died of symptoms similar to bird flu, Iraqi health officials said. Iraqi health authorities began killing domestic birds in northern Iraq, which borders Turkey, where at least 21 cases of the virus have been detected. Turkey and Iraq also lie on a migratory path for numerous species of birds. Abdul Qader died after contracting a lung infection in her village of Raniya, about 60 miles south of the Turkish border and just 15 miles west of Iran. Her mother rejected the bird flu results, but acknowledged that a number of her chickens had mysteriously died. The World Health Organization is putting together a crisis team to send to Iraq to conduct tests on the areas where the virus was found as well as people in hospitals exhibiting bird flu symptoms.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/30/AR2006013000370.html

29. *January 30, ComputerWorld* — **Efforts to track influenza are being hampered by incompatible systems.** The use of IT for tracking and potentially defeating a pandemic flu is being hampered by a lack of best practices, a need for more comprehensive state−of−the−art systems and the absence of a system to share data consistently from the actual sites of outbreaks, according to experts at the U.S. Centers for Disease Control and Prevention (CDC). In North America, agencies at the state, local, and federal levels use a wide variety of systems of differing degrees of sophistication to track influenza and share basic data among public health officials. Some of these are homegrown; others are "syndromic surveillance" applications −− dedicated systems created by third parties that track epidemics and help trigger a response from relevant agencies. Even with the information that's collected currently, the systems are unable to automatically do the requisite analysis and make the necessary recommendations to mount the most effective and aggressive response to stop a pandemic, say health officials. There are virtually endless ways to improve the existing surveillance systems, according to Lynette Brammer, epidemiologist for influenza at the CDC, which uses seven different applications to track flu outbreaks. At regional or municipal levels, there is a hodgepodge of new IT systems arrayed against the flu.
Source: http://www.computerworld.com/softwaretopics/software/story/0,10801,108096,00.html

30. *January 28, Agence France−Presse* — **U.S. medical centers seeking volunteers to test bird flu vaccine.** Medical centers in four states are seeking volunteers for the first human testing of a bird flu vaccine made by Chiron Corporation. Stanford Medical Center, in Palo Alto, CA, is one of four centers recruiting subjects to be injected with "inactive influenza A/H5N1 vaccine," said research assistant Ernesto Gonzalez. Stanford vaccine program director Cornelia Dekker said it will be the first time this particular vaccine is tested in humans. A Sanofi Pasteur bird flu vaccine was tested in human volunteers last year, with the August results showing that large doses triggered anti−body levels on par with those seen with common flu vaccines, Dekker

said. Since the Chiron and Sanofi vaccines are chemically similar, the testing being launched is focused on seeing whether chemicals called "adjuvants" can boost the potency, Dekker said. "The new study added two adjuvants in the mix to increase the immune response and make it possible to use less vaccine, and thereby have more doses for more people," Dekker said. A total of 280 subjects are being sought for testing at Stanford and medical centers in the states of Ohio, Tennessee, and Missouri. The trials are to begin in February.
Source: http://news.yahoo.com/s/afp/20060128/ts_alt_afp/healthfluusvaccine_060128153923;_ylt=Av2w.qAIF4mzVHeFyD8esZyJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

31. *January 30, Paradise Post (CA)* — **California county practices response to nerve agent release in water supply system.** Butte County, CA, officials conducted "Operation Silver Lining" Thursday, January 26 −− a drill in which officials had to inform and protect the public from a dangerous nerve agent that had infiltrated the water supply system. The scenario was used in a training session to organize the emergency operation centers (EOCs) that would be set up with Butte County, Paradise, Chico, Gridley and Oroville in the event of a disaster. The primary goal of the exercise was to establish communication lines between all of the EOCs. Steve Simpson, division chief of the Chico Fire Department, said it was difficult to pinpoint the actual source of the "contamination" because Feather River Hospital started having to divert patients to the Oroville Hospital. "Once that started happening, the staff had to make sure they knew where the patients were actually from," Simpson said. Several curveballs were also thrown at the EOCs, such as riots at the Kmart in Paradise after the store ran out of bottled water. By the end of the scenario, a joint information center supervised by the Federal Bureau of Investigation had been formed.
Source: http://www.paradisepost.com/local/ci_3447548

32. *January 29, Washington Post* — **Retailer Target branches out into police work.** When arson investigators in Houston needed help restoring a damaged surveillance tape to identify suspects in a fatal fire, they turned first to local experts and then to NASA. With no luck there, investigators appealed to the owner of one of the most advanced crime labs in the country: Target Corp. In the past few years, the retailer has taken a lead role in teaching government agencies how to fight crime by applying state−of−the−art technology used in its 1,400 stores. Target's effort has touched local, state, federal and international agencies. Besides running its forensics lab in Minneapolis, MN, Target has helped coordinate national undercover investigations and worked with customs agencies on ways to make sure imported cargo is coming from reputable sources or hasn't been tampered with. It has provided local police with remote−controlled video surveillance systems and linked police and business radio systems to

beef up neighborhood foot patrols in parts of several major cities. It has also linked city, county and state databases to keep track of repeat offenders. Target's law enforcement efforts date back at least a decade but intensified after the September 11, 2001, terrorist attacks.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/28/AR2006012801268.html

33. *January 29, Maine Today* — **Nursing homes in Maine have insufficient disaster plans.** Dozens of nursing home patients in New Orleans died after they failed to evacuate before Hurricane Katrina. Now emergency officials in Maine worry that outdated or inadequate disaster plans for similar facilities could put patients at risk. Some fire departments and emergency management officials are pushing for the plans to be reviewed before a crisis develops. Others have left the issue to individual nursing homes to address, when and if they choose. The state licenses nursing homes and conducts annual inspections, but it focuses more on quality of care than disaster planning. Fire drills are emphasized but inspections have failed to catch deficient disaster plans. Although state regulations say those plans must be filed with the state, that requirement is routinely ignored. There are 144 nursing homes with almost 7,500 patients in Maine. The extent of disaster planning and coordination by emergency officials varies widely across Maine. "Nobody does the planning until something happens," said Joanne Potvin, emergency management director for Lewiston/Auburn and Androscoggin County. For example, she said, a survey of the county's six nursing homes found three were using the same ambulance service to evacuate to the same location.
Source: http://pressherald.mainetoday.com/news/state/060129nursingho mes.shtml

34. *January 28, North County Times (CA)* — **California airport businesses have evacuation plans in place.** Many established businesses that line the perimeter of the McClellan−Palomar Airport in Carlsbad, CA, have evacuation plans in place to quickly move employees out of harm's way in the event of an emergency. For example, Callaway Golf Inc. conducts evacuation drills for fires and earthquakes twice a year, said Mike Majors, director of facilities for the Carlsbad−based golf equipment manufacturing company. Majors said all managers are trained in evacuation procedures, as are a team of employees on every shift. Kendal Floral, a bouquet distributor in the Palomar Airport Center business park, sits on the south side of the airport within about 40 yards of the runways. The company shares a fence with the airport, with planes parked within view of the company's shipping bay doors. Plant manager Jeff Sewell said the company consulted with architects in the design of the building in creating the evacuation plans. "I have seen an increased interest across the board among businesses to see how they can make their evacuation plans better," said Chris Heiser, Carlsbad Fire Department division chief. "It's great to see the public taking that ownership, and evacuation plans are a part of that."
Source: http://www.nctimes.com/articles/2006/01/29/news/coastal/20_3 4_081_28_06.txt

35. *January 27, News−Press (FL)* — **Florida counties' EOC buildings won't survive big hurricane.** There are more than 20 Florida counties, including Lee and Collier, in which the emergency operations centers (EOC) might not survive the worst hurricanes. Some are even in flood zones, according to a recent review by state officials. “These are not like tin sheds or shacks or anything,” said state Emergency Director Craig Fugate. “But...when we look at EOCs, we want the maximum protection.” The vulnerability has prompted Gov. Jeb Bush to ask legislators to put $70 million into shoring up county emergency operations centers next year. Collier County officials said they are well aware their emergency operations center

doesn’t meet safety standards for powerful hurricanes of Category 3 intensity or greater, said Jim von Rinteln, emergency management coordinator. Construction is scheduled to begin late this summer on a new $43 million center that will be better able to survive such storms, von Rinteln said. When finished, the building will house the county’s emergency operations, the 911 system, a sheriff’s substation and administrative offices for the county ambulance service. Source: http://www.news−press.com/apps/pbcs.dll/article?AID=/20060127/NEWS01/60127012/1075

[Return to top]

Information Technology and Telecommunications Sector

36. *January 30, Register (UK)* — **T−Mobile USA makes unprecedented network expansion.** The gap between T−Mobile USA and the other national carriers, Cingular, Verizon Wireless and Sprint Nextel, has widened following the past year’s wave of mergers in the U.S. mobile market. Now the German owned player is looking to narrow the gulf somewhat by expanding the reach of its network through roaming deals, as a preparation for likely more ambitious moves such as acquisitions of regional carriers and purchase of 3G spectrum in the next round of auctions. With the new roaming agreements, T−Mobile has extended the reach of its network by 56 percent, mainly through 850MHz partnerships that have put the carrier on a more competitive footing and mark a shift from its historic 1.9GHz−only platform. Most of the increase in footprint has been in the West, Midwest and rural Northeast through partnerships with carriers such as Alltel, Cingular, Centennial Communications, Dobson Communications, Edge Wireless and Rural Cellular. This has added more than 500,000 square miles of coverage. Source: http://www.theregister.co.uk/2006/01/30/t−mobile_us_plan/

37. *January 27, Federal Computer Week* — **Experts: Countries make dangerous cyber adversaries.** When other countries launch cyber attacks, the United States should expect to see more robust ways to crack systems and more dangerous methods to manipulate them, two cybersecurity experts said Thursday, January 26. Countries have many resources and can attack at least as effectively as independent cybercriminals can, said Matthew Devost, president and chief executive officer of the Terrorism Research Center. China, North Korea and Russia already use cyber attacks to advance their interests, Devost said, speaking on a panel at the Black Hat Federal conference in Arlington, VA. Cyber attacks from countries can be difficult to investigate because analysts may not be able to tell if a given country is launching the attack or if other organizations are attacking through the country’s resources, he said. Countries and terrorist organizations can have a different perception of time than other cyber attackers do, Devost said. They can wait years, performing reconnaissance and placing agents inside target organizations to find vulnerabilities, he said. Preparation is important to stopping attacks from other countries, said Tom Parker, security research group manager at MCI. Organizations must anticipate their adversaries’ actions and look at all data, attack profiles and threat types, he said. Source: http://www.fcw.com/article92121−01−27−06−Web

38. *January 27, Register (UK)* — **New legislation criminalizes social engineering.** New legislation proposed by Senator Chuck Schumer (D−NY) and backed by both major parties, seeks to criminalize both the practitioners and the dupes of "social engineering." Social engineering is a way of smooth−talking someone out of information they shouldn't normally

impart, but it has been the most effective technique for scammers, hackers and private eyes over the years. Schumer's bill, the proposed Consumer Telephone Records Protection Act of 2006, makes disclosing a subscriber's phone records an offense. It specifically outlaws making false statements or providing phony documentation to a phone provider in order to obtain the records, and accessing an account over the Internet without the subscriber's authorization. According to the Electronic Privacy Information Center, over 40 Websites including celltolls.com and locatecell.com have been trading in a black market in call records.
Source: http://www.theregister.com/2006/01/27/schumer_phone_records/

39. *January 27, Associated Press* — **Man sentenced for stealing Microsoft code.** A Connecticut man known on the Internet as "illwill" was sentenced to two years in prison Friday, January 27, for stealing the source code to Microsoft Corp.'s Windows operating software, among the company's most prized products. William Genovese Jr., 29 of Meriden, CT, was sentenced by U.S. District Judge William H. Pauley, who called Genovese "a predator who has morphed through various phases of criminal activity in the last few years." Genovese pleaded guilty in August to charges related to the sale and attempted sale of the source code for Microsoft's Windows 2000 and Windows NT 4.0. The code had previously been obtained by other people and unlawfully distributed over the Internet, prosecutors said. Source code is the blueprint in which software developers write computer programs. With a software program's source code, someone can replicate the program. Industry experts expressed concern that hackers reviewing the Microsoft software code could discover new ways to attack computers running some versions of Windows. Prosecutors said in an indictment in February 2004 that Genovese posted a message on his Website offering the code for sale on the same day that Microsoft learned significant portions of its source code were stolen.
Source: http://news.yahoo.com/s/ap/20060128/ap_on_hi_te/microsoft_source_code;_ylt=Am2Q37WFib1DhYnAQZ9D.JEjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

40. *January 27, Associated Press* — **Maryland spam law can be enforced, judge rules.** Spam e−mails offering home financing deals or other offers can violate Maryland law, even if they're sent from another state, a state appeals court has ruled. Court of Special Appeals Judge Sally D. Adkins sided with a law student who argued that he could sue a New York e−mail marketer who had sent him advertising messages. The decision, issued Thursday, January 26, overturns a lower court ruling that Maryland's 2002 Commercial Electronic Mail Act was unconstitutional because it sought to regulate commerce outside state borders. Adkins, in a 60−page decision, blasted the marketer's claims that he should not be punished for violating Maryland law because he had no way of knowing whether his e−mails would be opened in Maryland. "This allegation has little more validity than one who contends he is not guilty of homicide when he shoots a rifle into a crowd of people without picking a specific target, and someone dies," the judge wrote. Maryland was one of the first states to try to control junk e−mail through legislation, and its 2002 law predates the 2004 federal CAN−SPAM Act. The federal law superseded most state laws unless they specifically addressed deceptive or fraudulent e−mail, which Maryland's does.
Source: http://www.siliconvalley.com/mld/siliconvalley/news/editoria l/13728469.htm

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 receiving reports of a new destructive email worm known as CME 24, which will actively disable anti−virus software on a host system and will also overwrite users' data files on the third of every month. This worm affects all recent versions of Microsoft Windows. CME 24 is also known as Nyxem.E, Blackmal.E, MyWife.d, BlackWorm, Tearec.A, Grew.a, and Kama Sutra.

This malcode spreads primarily by harvesting email addresses from files on the local machine and then emailing itself as an executable attachment. It uses subject lines such as "Photos", "*Hot Movie*", and "Miss Lebanon 2006" to entice the user into opening the attachment. As soon as the attachment is executed, the user's system is immediately infected. Infected hosts within a network enclave will also try to spread locally through network shares with weak passwords.

On the third of every month, CME 24 will over−write users' files on all accessible drives with the message "DATA Error [47 0f 94 93 F4 F5]". This will happen approximately 30 minutes after the user logins to the infected machine. The files affected by this variant will have the following file extensions: .doc, .xls, .mdb, .md3, .ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp.

The infected host will also access a website containing a counter. The web counter shows how many machines have been infected, although it is expected that an infected machine may access that website on multiple occasions, thus inflating the number. The web counter has shown consistent growth with over 500,000 infections on Saturday and is now currently showing over 700,000 infections. FBI agents have received log data that resided on the web server, and is sharing the bulk data with US−CERT for analysis.

As CME 24 disables anti−virus systems, it leaves infected computers wide open to attack by other malware variants. All major anti−virus companies are offering signature files that should prevent infection. In addition, major anti−virus vendors are offering tools and instructions for removing this variant from their systems. v US−CERT has not received any reports of infections within the Federal space. Currently, US−CERT is coordinating the analysis of log file data that could be an indicator of infected systems, and will be distributing notifications to affected parties.

Nyxem Mass−mailing Worm US−CERT is aware of a new mass mailing worm known as Nyxem (CME−24). This worm relies on social engineering to propagate. Specifically, the user must click on a link or open an attached file.The Nyxem worm targets Windows systems that hide file extensions for known file types (this is the default setting for Windows XP and possibly other versions). The worm's icon makes it appear to be a WinZip file. As a result, the user may unknowingly execute the

worm. For more information please review: http://cme.mitre.org/data/list.html#24

US−CERT strongly encourages users not to follow unknown links, even if sent by a known and trusted source. Users may also wish to visit the US−CERT Computer Virus Resources for general virus protection information at URL: http://www.us−cert.gov/other_sources/viruses.html

Current Port Attacks

Top 10 Target Ports	4556 (−−−), 1026 (win−rpc), 6881 (bittorrent), 6346 (gnutella−svc), 445 (microsoft−ds), 25 (smtp), 139 (netbios−ssn), 32768 (HackersParadise), 49200 (−−−), 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

41. *January 30, St. Louis Post−Dispatch (MO)* — **Missouri city considers camera surveillance.** Officials seeking to revive Granite City's downtown business district are considering using public security cameras, possibly with motion sensors. After studying other surveillance systems, Mayor Ed Hagnauer said he likes what he sees. For example, in St. Louis, police have used portable cameras to target high crime areas and street festivals. "What we're trying to deter are people being confronted with the prostitution and drugs," Hagnauer said. "And if people are hesitating to do anything with their properties like repairs or investments, we need to change that." The city is looking at purchasing four security cameras at $15,000 each. A resolution is expected to be considered at the council meeting on February 7. "Cameras give us the ability to watch and gather evidence and prosecute," said Granite City Police Chief Rich Miller.
Source: http://www.stltoday.com/stltoday/news/stories.nsf/metroeast/story/971EF3D0E1FB445E86257106002008B7?OpenDocument

42. *January 29, Associated Press* — **Lawmakers reconsider audio surveillance on school buses.** New Hampshire lawmakers are considering for a second time whether to allow school districts to record audio as well as video on school buses. Rep. Stephen L'Heureux (R−Hooksett), tried unsuccessfully to get similar legislation passed last year but lost to those who felt the audio recordings were an invasion of privacy. "We addressed that issue by saying someone viewing the tape looking for a specific incident cannot use anything not relevant to that incident to be used against the kid," L'Heureux said. "The whole idea of putting audio on a bus is because now you just have video and when you see two kids fighting, you don't hear if there are two other kids instigating the fight. The bus driver may say there's four kids involved, but there's no proof." The bill would require school boards that are considering installing recording devices to hold public hearings to get input from parents on who should be allowed to view or listen to the recordings. Also included in the bill is a provision that all tapes must be destroyed after 10 days, unless a court proceeding or other disciplinary action is ongoing.
Source: http://www.seacoastonline.com/news/special/1_29special4.htm

[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