Department of Homeland Security Daily Open Source Infrastructure Report for 06 January 2006

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

Daily Highlights

- The Associated Press reports a Frontier Airlines passenger who had a notebook that contained the words "suicide bomber" was taken into custody and questioned for several hours before being released to his family in California. (See item 8)
- The Washington Post reports a Virginia Railway Express engine and three train cars carrying 400 passengers derailed just north of Quantico, Virginia, early Thursday, January 5, injuring five people, and blocking two train tracks. (See item 13)
- Reuters reports Swiss drug maker Roche Holding AG says it has stepped up distribution of its Tamiflu flu treatment to wholesalers serving U.S. markets that have reported a high incidence of influenza. (See item 21)

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. *January 05, Boston Globe (MA)* — **Alliance formed to push for increased electricity to prevent threat of rolling blackouts.** Nearly two−dozen top officials from business, labor unions, and academia have formed a group called the Massachusetts Affordable Reliable Electricity Alliance to push for expanded in−state supply of electricity. The group intends to

highlight the importance of reliable power as regional electric−grid officials increasingly threaten rolling blackouts to cope with tight supplies. The alliance includes officials from Associated Industries of Massachusetts, Local 369 of the Utility Workers Union of America, Duke Energy, and Entergy Corp.
Source: http://www.boston.com/business/globe/articles/2006/01/05/alliance_formed_to_push_for_increased_electricity/

2. *January 05, The News & Observer (NC)* — **Nuclear Regulatory Commission to probe nuclear plant security.** The Nuclear Regulatory Commission (NRC) will conduct interviews next week at Shearon Harris Nuclear Plant to see whether they can verify allegations of lax security at the plant located near Raleigh, NC. According to Ken Clark, NRC spokesperson: "This is a special inspection related to concerns that have been raised about inadequate security measures at the plant...The NRC staff has not reached any conclusions as to the validity of the concerns. But we are still looking into it, and we are seeking information." A complaint filed in December by Waste Awareness and Reduction Network (WARN) and the Washington−based Union for Concerned Scientists, alleged lapses in security at the nuclear plant. Owner Progress Energy rejects the charges and have said that the plant is safe and secure. The complaint alleged that guards, employed by an outside security firm, have been forced to cheat on guard re−licensing tests, made to work while injured, retaliated against for reporting injuries, and allowed to sleep on their shifts. WARN's source of information was an unidentified guard at the Shearon Harris plant. The complaint also contends that the plant has some inoperable intruder detection equipment and doors with worn−out hardware that keeps them from locking properly.
Source: http://www.newsobserver.com/102/story/384961.html

3. *January 05, Boston Globe* — **Evacuation plan is termed inadequate at Massachusetts nuclear plant.** A Plymouth, MA, report on safety concerns at the Pilgrim nuclear power plant says the town has grown so much in the 30 years of the plant's existence that the "current evacuation plans do not pass any reasonable reality check." School buses evacuating children during a radioactive emergency at Pilgrim would get stuck in traffic, and bus drivers may not even show up, according to the report released Tuesday, January 3, by the town's Nuclear Matters Committee. Plymouth elected officials say the Entergy Corp., which owns Pilgrim, needs to pay for a new evacuation plan, compensate the town because the plant generates nuclear waste that could be the target of terrorists, and pay higher property taxes. In an emergency, the report said, some residents may not be aware of the need to evacuate because the warning sirens in Plymouth, a town of 54,000, are not loud enough for all to hear. The report recommends that the town select specialists to prepare a new evacuation plan, which Entergy should pay for. The report also criticized the nuclear fallout shelter system in place, community education on nuclear issues, and potential spent nuclear fuel storage problems.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/01/05/plymouth_asks_more_of_nuclear_plant/

4. *January 04, U.S. Department of Labor* — **Federal mine safety agency launches accident investigation.** On Wednesday, January 4, the U.S. Department of Labor's Mine Safety and Health Administration (MSHA) launched its investigation into the underground coal mine explosion that killed 12 miners and seriously injured one additional miner. The blast occurred on Monday, January 2, at the Sago Mine in Upshur County, WV. The mine was acquired last year by International Coal Group Inc. According to David G. Dye, acting assistant secretary for

mine safety and health: "The purpose of MSHA's investigation is to determine what caused the explosion and whether any safety and health standards were violated...Then we can take effective action to prevent such tragedies in the future." An independent team of MSHA mine safety professionals will evaluate all aspects of the accident and response, including potential causes, compliance with federal health and safety standards, and how emergency information was relayed about the trapped miners' condition. The team will examine the accident site, interview mine personnel and others with relevant information, review records and plans, and inspect any mining equipment that was involved in the accident. Findings and conclusions will be summarized in a formal report that will identify root causes of the accident and document how the incident unfolded.
Source: http://www.dol.gov/opa/media/press/msha/MSHA200618.htm

5. *January 04, Associated Press* — **Report: Michigan will need more electricity as early as 2009.** Demand for electricity in Michigan will be too much for the current system in three years and will require at least one more power plant in the state by 2014, according to a report released Wednesday, January 4. Demand for power will grow by about two percent a year, according to the Michigan Public Service Commission (PUC). The state's generation and transmission system will need improvements as early as 2009 to keep up with demand in the Lower Peninsula. The report suggests renewable energy and combined heat and power systems to boost supply. According to J. Peter Lark, chairman of the Michigan PUC, "With aging electric plants and increasing demand for electricity, Michigan needs to start planning now to ensure that the lights stay on well into the future." The Public Interest Research Group in Michigan (PIRGIM), an Ann Arbor−based watchdog organization, disputed the forum's projections that more power plants would be needed in the near future. PIRGIM Director Mike Shriberg said the state should implement policies that better conserve energy and use renewable energy sources rather than building new coal−fired power plants.
Report: http://www.dleg.state.mi.us/mpsc/electric/capacity/cnf/cnf_r eport_1−3−06.pdf
Source: http://www.centredaily.com/mld/centredaily/business/13548274 .htm

6. *January 04, Associated Press* — **New view on wind energy enhances resource reliability.** A group of Iowa cities intends not only to harness the wind, but also capture it, store it underground, and use it to help make electricity when demand peaks. Members of the Iowa Association of Municipal Utilities have invested in a proposed power plant that would use wind turbines to drive compressed air into underground aquifers. The air would be released to generate electricity when needed. It's a new twist on the idea of using wind energy in a way that removes the unreliability of nature. The project, backed by 74 members of the municipal utilities group, obtained a $1.2 million U.S. Department of Energy grant last year to study the idea. It anticipates another one million this year to continue to evaluate the project's feasibility. About $700,000 has been raised by the utilities that support the idea. Only two other underground compressed air plants are in operation. Iowa's project is unique in that it would use wind power to store the air and combine it with massive underground storage capacity.
Source: http://www.msnbc.msn.com/id/10695864/

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

7. *January 05, INQ7−Net (Philippines)* — **Mobile malware, phishing activities to surge in 2006.** According to the McAfee AVERT (Anti−Virus and Emergency Response Team) Labs, the rapid evolution of smart−phone technology and the growing use of converged mobile devices will fuel the rise in the number of mobile malware in 2006. The perception that the threat of mobile malware was much less than that of its PC counterpart would encourage virus writers to come up with even more sophisticated threats, the McAfee AVERT Labs added. The McAfee AVERT Labs said that since the inception of malware, mobile malware had grown ten times faster than its PC counterparts over a one−year period. The company said the number of distributed phishing Trojans, or Trojans that turn infected computers into phishing Websites that, in turn, spam other computers to go to that infected machine or site, would also increase in 2006. More scammers were also expected to take advantage of people's kindness and willingness to help others in need, the firm said, as proven by the influx of phishing attacks following Hurricane Katrina. While attacks on Internet service providers were expected to decline, those targeted at the financial sector would remain steady, the company said.
   Source: http://news.inq7.net/infotech/index.php?index=1&story_id=620 81

[Return to top]

Transportation and Border Security Sector

8. *January 05, Associated Press* — **Passenger taken into custody at California airport, later released.** A Frontier Airlines passenger on a flight from Denver who had a notebook that contained the words "suicide bomber" was taken into custody Wednesday, January 4, and questioned for several hours before being released to his family, police said. The suspect, a 36−year−old male, got the attention of a fellow passenger after writing in a journal that had the words "suicide bomber" handwritten on the front, authorities from the San Jose Police Department and the FBI said. He was also clutching a backpack in what the fellow passenger regarded as a suspicious manner. The man was taken from Frontier Flight 169 after it taxied to a halt on the tarmac at Mineta San Jose International Airport, stopping just short of the gate. He was questioned by the FBI and San Jose police, who were in charge of the investigation, authorities said. A final decision about whether to file charges probably will not be made for another two weeks. Police confiscated the journal and still have it in their possession. "It seemed like he was under the influence but that's not been determined at this point," said Patty Hansen, a spokesperson at the FBI.
   Source: http://www.usatoday.com/travel/news/2006−01−05−flier−detaine d_x.htm

9. *January 05, Associated Press* — **Northwest flight attendants threaten strike if contract voided.** Northwest Airlines' flight attendants union says in a bankruptcy filing that it may strike if a bankruptcy judge allows the carrier to reject its contract. Eagan, MN−based Northwest is negotiating with pilots, flight attendants and ground workers ahead of a January 17 hearing in which the nation's fourth−largest airline will ask to reject their contracts. Northwest has said it wants to use more foreign−based flight attendants on international flights and use flight attendants at a new subsidiary on smaller domestic flights. Northwest Airlines filed for Chapter 11 bankruptcy protection September 14. Bankruptcy law allows it to seek to overturn union contracts as part of its reorganization. Northwest has said such a strike would be illegal, but the unions have said the issue of whether they can strike during bankruptcy has not been tested in the courts.
Source: http://www.usatoday.com/travel/news/2006−01−05−nwa−attendant s_x.htm

10. *January 05, Associated Press* — **Atlanta's airport is busiest in the world.** Hartsfield−Jackson Atlanta International Airport has topped Chicago O'Hare International Airport as the nation's busiest in terms of takeoffs and landings, the Federal Aviation Administration (FAA) said Tuesday, January 3. The Atlanta airport also is considered the busiest in the world. Hartsfield−Jackson finished 2005 with 980,197 takeoffs and landings, while O'Hare was second with 972,246. A possible explanation for the surge at the Atlanta airport is fleet and operational changes at Delta Air Lines Inc., which has its hub in Atlanta. The airline, which filed for bankruptcy protection in September, has shifted more flights to Atlanta after shuttering its hub in Dallas and scaling back operations in Cincinnati. In addition, the FAA and O'Hare's major airlines agreed in August 2004 to cut the number of flights at the delay−prone facility, which had the worst delays of the nation's 31 busiest airports in 2004. Under the restrictions, which are scheduled to expire in April, United Airlines and American Airlines agreed to cut 37 daily peak−hour flights.
Source: http://www.usatoday.com/travel/flights/2006−01−04−atlanta−ch icago_x.htm

11. *January 05, CNN* — **A voice analyzer for airborne criminals.** Heightened fears of terrorist attacks have lead to a global increase of airport security, and additional new measures are being developed that could see plane passengers screened by lie detectors. Now a new walk−through airport "lie detector" developed by Israeli scientists could add yet another layer of security to ensure that potential hijackers or contraband smugglers do not gain access to international flights. The GK−1 voice analyzer requires passengers to don headphones at a console and answer "yes" or "no" into a microphone to questions about their travel plans. The manufacturers say the device, which will cost between $10,000 to $30,000, will usually be able to pick up uncontrollable tremors in the voice that give away liars or those with something to hide. Those that fail the screening are led away for more in−depth questioning and, if necessary, searches. Nemesysco CEO Amir Liberman says the device has proved highly successful in tests, but admits that the results can sometimes be difficult to interpret with around 12 percent of passengers likely to show stress even when they have nothing to hide.
Source: http://www.cnn.com/2006/TRAVEL/01/05/lie.detectors/

12. *January 05, Reuters* — **U.S. agents shot at, tension mounts on Mexico border.** U.S. Border Patrol agents have come under fire twice along the Rio Grande in Texas in recent days amid rising tension on the frontier with Mexico, although no one was reported wounded, U.S. authorities said on Thursday, January 5. A Border Patrol spokesperson said unknown gunmen

fired on agents on patrol in Brownsville, TX, late on Wednesday, January 4. "Shots were fired, no one was injured and the FBI have taken the case over," Jose Rodriguez, a spokesperson for the Border Patrol in McAllen, TX, said by telephone. Rodriguez said the shooting was the second along the same stretch of the Rio Grande in the past week, after agents patrolling the area in a launch on Friday, December 30, came under a volley of gunfire from Mexico. "On that occasion the shooters were hiding in brush on the Mexican side of the river ... The launch was struck by five bullets, although there were no injuries," he said. That incident came on the same day a Border Patrol agent fatally shot a teenage Mexican immigrant as he crossed the border near San Diego, triggering widespread anger in Mexico and calls for a full investigation.
Source: http://today.reuters.com/news/newsarticle.aspx?type=domesticNews&storyid=2006−01−05T183209Z_01_SIB566190_RTRUKOC_0_US−MEXICO−USA.xml&rpc=22

13. *January 05, Washington Post* — **Virginia train derails, injuring five.** The engine and three cars of a train carrying 400 passengers derailed just north of Quantico, VA, in Prince William County early Thursday, January 5, as the region was draped in fog, injuring five people, fire and rescue officials said. Virginia Railway Express (VRE) train No. 304 jumped the tracks just before 7 a.m. EST, said Capt. Tim Taylor, spokesperson for Prince William County fire and rescue services. "The train stayed upright after it derailed, minimizing injuries on site," Taylor said. He said the train was carrying 400 passengers and three crewmembers. All train traffic in the area has been halted, Taylor said, creating a major headache for train commuters. VRE cancelled trains Nos. 306, 308, and 310 out of Fredericksburg after the derailment, advising passengers to find alternative forms of transportation. Amtrak also suspended service between the District and Richmond, according to VRE spokesperson Mark Roeber. "All traffic on the Fredericksburg line is halted because the train is blocking both tracks," Roeber said. He said thousands of train commuters will be affected by the derailment since each train can hold 800 to 900 people.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/05/AR2006010500491.html

[Return to top]

Postal and Shipping Sector

14. *January 05, Government Computer News* — **USPS seeks help as it reviews encryption policies.** The U.S. Postal Service (USPS) is reaching out to industry as it undertakes a broad review of its data encryption policies. In a January 4 sources−sought notice, USPS said it wants vendors to provide information about their encryption products that may help it develop an enterprise−wide program. USPS said technology changes have forced it to consider changes as to how it protects sensitive information, and responses to the notice must propose solutions that can protect data ranging from physical tapes that will be removed from its auspices to information on the agency's controlled storage devices.
Source: http://www.gcn.com/vol1_no1/daily−updates/37895−1.html

[Return to top]

Agriculture Sector

15. *January 05, Associated Press* — **Researchers explore timber aroma tags.** Timber researchers hope to create wood sniffers that could track lumber from forest to front−room furniture by their scent. They could make it harder to move pirated logs, reducing theft and illegal logging. Or they could help the industry be better at marketing and management. Glen Murphy, a forest engineering professor at Oregon State University, says he envisions an electronic "wood hound." Lumber would be tagged with scents such as the three perfumery chemicals he's been using on wood samples from cedar, ponderosa pine, and hemlock trees. So far, the $8,000 device he's using can track one distinct scent, but it can't deal with combinations of more. Five years from now, Murphy hopes to be able to track 25 aromas in various combinations. That would allow timber trackers to tag more than 33 million logs with a unique scent for each, he said. "Ideally, we want to track from standing tree to piece of wood on a desk," he said. "That's where we want to go. A smell is like a fingerprint." The industry now uses metal staples or plastic tags that play hob with pulp mill and sawmill machinery. The alternative is radio frequency tags, which are expensive.
Source: http://www.sunherald.com/mld/sunherald/news/breaking_news/13 550499.htm

[Return to top]

Food Sector

16. *January 05, Associated Press* — **Chicken industry plans to test flocks.** Chicken companies intend to test every chicken flock in the U.S. for bird flu before slaughter, an industry group said Thursday, January 5. The U.S. produced more than 9.5 billion chickens in 2005. The National Chicken Council said companies that make up more than 90 percent of the nation's production have signed up for testing and that more are expected to follow. The U.S. produced more than 9.5 billion chickens in 2005. The testing program, which the industry will finance, calls for 11 birds to be tested from each chicken flock, or farm. There are an estimated 150,000 flocks produced each year, which would mean around 1.6 million chickens would be tested. Samples will be collected on farms and tested at state or industry−certified laboratories. If testing indicates highly pathogenic bird flu is present and results are confirmed by the U.S. Department of Agriculture the flock will be destroyed on the farm. None of the birds from the affected farm will enter the food chain, the council said.
Source: http://www.usatoday.com/news/health/2006−01−05−chicken−testi ng_x.htm

[Return to top]

Water Sector

17. *January 05, State−Journal Register (IL)* — **Carlinville man, three companies indicted in pollution case.** A Carlinville, IL, man was indicted Wednesday, January 4, along with three companies for allegedly dumping wastewater contaminated with boron into a tributary of the Sangamon River without having the proper paperwork to do so. If convicted, the penalty for violation of the federal Clean Water Act is up to three years in prison and a fine of $5,000 to $50,000 a day each day of the violation. According to the U.S. attorney’s office, ash from a

utility company had been put in an excavation at the North Dirksen address. Excess levels of boron leached from the ash into water that had accumulated in the excavation. According to the indictment, the concentration of boron in the water was 13 times higher than allowed. It also alleges that between March and June of 2003, an employee of the companies, discharged a large portion of several million gallons of the contaminated water by pumping it into a trench that led to a drain that emptied into the tributary and through a hose that emptied on the bank of the tributary.
Source: http://www.sj−r.com/sections/news/stories/75428.asp

[Return to top]

Public Health Sector

18. *January 05, Bloomberg* — **Turkey's bird−flu deaths bring virus to the threshold of Europe.** Turkey said a second teenager infected with avian flu died, indicating the virus that's killed at least 74 people since 2003 has moved outside East Asia to the threshold of Europe. A 15−year−old girl who died Thursday, January 5, and her 14−year−old brother who died on Sunday, January 1, both had avian flu, said Huseyin Avni Sahin, chief physician at the hospital where the children died. The hospital, in the eastern city of Van, is treating nine others suspected of having the H5N1 strain of the virus. The deaths come less than two weeks after Turkey reported a second wave of avian flu in poultry and mark the virus's westward progression from China and Southeast Asia. All 11 of Turkey's suspected cases, including the siblings who died, are from Dogubeyazit, a town on the Iranian border, and came into contact with chickens that died of unknown causes, hospital officials said. The virus was confirmed last week in birds in a town 50 miles north of Dogubeyazit. The town is about 932 miles away from the European continent in the easternmost corner of Turkey.
Source: http://www.bloomberg.com/apps/news?pid=10000082&sid=a3k_X9kqnQ3g&refer=canada

19. *January 05, Infection Control Today* — **Drug−resistant bacteria patterns in intensive care units changing nationally.** A drug−resistant bacterium is becoming more prevalent in many intensive care units. Methicillin−resistant Staphylococcus aureus (MRSA) is responsible for a variety of infections that patients often acquire in the hospital. Skin infections are the most common, but MRSA can also infect the heart, the lungs, and the digestive tract. Researchers at the Centers for Disease Control and Prevention (CDC) examined MRSA data from more than 1,200 intensive care units (ICUs) from 1992 to 2003. They found that in 1992, 36 percent of S. aureus isolates were drug−resistant; but in 2003, 64 percent of isolates were MRSA, an increase of about three percentage points per year. Despite the increase in MRSA prevalence, there was also a decrease in MRSA that was resistant to multiple drugs. The researchers hypothesize that the influx of MRSA strains from the community might have replaced those multidrug−resistant strains associated with the hospital. "Unlike traditional MRSA the community strain is very fit −– it causes infection in healthy people," said CDC epidemiologist Monina Klevens. "When it is introduced into a hospital, where ill patients are more vulnerable to infection, it has the potential to cause significant morbidity and mortality."
Abstract: http://www.journals.uchicago.edu/CID/journal/issues/v42n3/38050/brief/38050.abstract.html
MRSA information: http://www.cdc.gov/ncidod/diseases/submenus/sub_mrsa.htm

Source: http://www.infectioncontroltoday.com/hotnews/61h58371510333. html

20. *January 05, SciDev.Net* — **United Nations plans bird flu alert system for North Africa.** The United Nations' Food and Agriculture Organization (FAO) has approved plans to create an early warning system to alert North African countries of outbreaks of the deadly bird flu virus, H5N1. The plans, agreed upon on December 24, will be implemented through the FAO's Technical Cooperation Program and will cover Algeria, Egypt, Libya, Mauritania, Morocco, and Tunisia. The FAO has warned that migratory birds could bring the virus to Africa from parts of Asia and Eastern Europe where outbreaks have been reported. Many migrating birds pass along the River Nile, where most of Egypt's population lives. Birds also use Algeria and Morocco as stop−overs during their flight to warmer places further south. National action plans for combating bird flu will also be prepared through the initiative.
Source: http://www.scidev.net/gateways/index.cfm?fuseaction=readitem&rgwid=2&item=News&itemid=2570&language=1

21. *January 04, Reuters* — **Roche says it stepped up U.S. Tamiflu distribution.** Swiss drug maker Roche Holding AG said on Wednesday, January 4, it has stepped up distribution of its Tamiflu flu treatment to wholesalers serving U.S. markets that have reported a high incidence of influenza. Roche said it would continue to meet seasonal demand for the prescription antiviral medicine, also known by the chemical name oseltamivir phosphate, and work with governments to supply stockpiles of the drug in preparation for any potential flu pandemic. Tamiflu can reduce the duration and severity of the flu if taken within two days of the onset of symptoms. Demand for the drug has soared amid fears that the avian flu that has caused more than 70 human deaths in Asia could turn into a major flu pandemic. Roche said it has implemented an inventory management plan to ensure adequate supplies would be available for seasonal flu demand. The company said Tamiflu will continue to be shipped where it is needed.
Source: http://today.reuters.com/business/newsArticle.aspx?type=health&storyID=nN04375462

22. *January 04, National Institutes of Health* — **Structure of viral harpoon protein reveals how viruses enter cells.** A team of Northwestern University researchers has solved the structure of a molecule that controls the ability of viruses of the paramyxovirus family, including the viruses that cause measles, mumps, and many human respiratory diseases, to fuse with and infect human cells. Determining the structure of this molecule and its role in the viral fusion mechanism may aid the development of drugs and vaccines that target these types of viruses, say the scientists, whose work was funded by the National Institute of General Medical Sciences and the National Institute of Allergy and Infectious Diseases, both parts of the National Institutes of Health. This large protein, called F, studs the surfaces of certain RNA viruses that are encased in a membrane envelope. As soon as such a virus comes in contact with a cell it can infect, the F protein changes shape and extends like a harpoon into the outer membrane of that cell. Then the protein undergoes a conformational (shape) change and collapses upon itself, pulling the virus against the host cell, and fusing the viral membrane with the target cell's membrane. The fusion unleashes the viral RNA into the cell, which then hijacks the cell's machinery to make and spread more virus.
Source: http://www.nih.gov/news/pr/jan2006/nigms−04.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

23. *January 04, East Aurora Advertiser (NY)* — **Emergency responders prepare for serious disaster in New York.** East Aurora, NY, emergency responders and officials have tried to prepare for their response to a serious disaster through in series of meetings over the past six months. East Aurora is prone to a major disaster because it is a unique population center where major transportation corridors meet, said Craig Thrasher, a member of the East Aurora Fire Department. East Aurora is also home to a 36−inch high−pressure natural gas pipeline and high−voltage power lines. Through a series of four sessions over the past six months, emergency responders have brought together local officials and schools to rehearse their individual roles in the event of a disaster. "It's been a very successful exercise," Thrasher said of the meetings, which included a simulated disaster drill at the East Aurora Fire Hall on Wednesday, December 7. In a tabletop exercise, participants rehearsed their response to the hypothetical train derailment. In the event of such a disaster, an emergency operations center would be established to coordinate the response efforts among village, town, county and school officials using nationally developed procedures. The simulation, Thrasher said, helped participants better understand the available communication systems and foster a sense of teambuilding to solve unexpected events.
Source: http://www.zwire.com/site/news.cfm?newsid=15867808&BRD=984&PAG=461&dept_id=141126&rfi=6

24. *January 04, Denver Post (CO)* — **Location technology for wireless 911 callers lags in Colorado.** Colorado is behind most states when it comes to having the technology to pinpoint the location of wireless 911 callers. As of Tuesday, January 3, only a third of Colorado counties had the capability to identify the callback number and location of a wireless caller within 50 to 100 meters. The national average of counties that have that capability is 44 percent, and some states, such as Tennessee, Minnesota and Vermont, have 100 percent coverage. "Colorado is one of the states that is lagging," said Patrick Halley, government affairs director of the National Emergency Number Association (NENA), a nonprofit agency dedicated solely to 911 emergency communication issues. In addition, Halley said, Colorado does not have a state 911 coordination entity of some kind, which helps advance 911 systems and is in place in 34 other states. Colorado's state NENA president, Collet Daubenspeck, said the problem is keeping up with ever−changing phone systems, such as Voice over Internet Protocol (VoIP) where voice conversations are routed over the Internet, or any other IP−based network. Many of those systems are not designed to handle 911 calls, Daubenspeck said, and collect no surcharges from their customers toward that end.
Source: http://www.denverpost.com/news/ci_3369070

25. *January 04, GovExec* — **New Preparedness Directorate at the Department of Homeland Security up and running.** In one of its first official acts, the Department of Homeland

Security's (DHS) new Preparedness Directorate on Tuesday, January 3, issued preliminary guidelines for emergency responders to follow in the event of a radiological or nuclear attack. Homeland Security Secretary Michael Chertoff announced the creation of the directorate last year as part of a broad restructuring of the department. The Senate last month confirmed George Foresman, who served as assistant to the governor of Virginia for emergency and disaster preparedness, as head of the directorate. The directorate is officially up and running, DHS spokesperson Marc Short said Wednesday, January 4. According to an organizational chart, the directorate includes a chief medical officer, the U.S. Fire Administration, a National Capital Region director and assistant secretaries for grants and training; infrastructure protection; and cyber and telecommunications. The draft guidelines published Tuesday represent the government's first comprehensive attempt to outline what responders should do during the early, intermediate and late stages of an attack from a radiological dispersal device, or an improvised nuclear devise. These guidelines are intended to help decision−makers determine appropriate courses of action, which may include using procedures already established by other agencies, said DHS spokesperson Larry Orluskie.
Source: http://govexec.com/story_page.cfm?articleid=33092&dcn=todays news

[Return to top]

Information Technology and Telecommunications Sector

26. *January 04, FrSIRT* — **ESRI ArcPad ".apm" file handling remote buffer overflow vulnerability.** A vulnerability has been identified in ESRI ArcPad, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a buffer overflow error when processing malformed ".amp" files containing an overly long "COORDSYS" string attribute, which could be exploited by attackers to compromise a vulnerable system by convincing a user to open a specially crafted "apm" file. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2006/0032

27. *January 04, FrSIRT* — **Linux Kernel multiple denial of service and privilege escalation issues.** Multiple vulnerabilities were identified in Linux Kernel, which could be exploited by malicious users to cause a denial of service and potentially obtain elevated privileges. The first issue is due to an error in "mm/mempolicy.c" when handling policy system calls, which could be exploited by local attackers to cause a denial of service via a "set_mempolicy" call with a 0 bitmask. The second flaw is due to a one−byte buffer overrun error in "kernel/sysctl.c" when processing an overly long user−supplied string, which could be exploited by local attackers to potentially execute arbitrary commands. The third vulnerability is due to an error in "net/ipv4/fib_frontend.c" when processing malformed "fib_lookup" netlink messages, which could cause illegal memory references. The fourth issue is due to a buffer overflow error in the CA−driver for TwinHan DST Frontend/Card [drivers/media/dvb/bt8xx/dst_ca.c], which could be exploited by malicious users to cause a denial of service or potentially execute arbitrary commands. Solution: Upgrade to Linux Kernel version 2.6.15: http://www.kernel.org/.
Source: http://www.frsirt.com/english/advisories/2006/0035

28. *January 04, CNET News* — **Experts: Sober time bomb's under control.** The Sober attack expected later this week is unlikely to have much effect on company systems, antivirus experts

predicted. As reported last month, machines that were infected by Sober in November have the potential to download malicious code from certain Websites and then launch a new wave of viruses on Thursday, January 5, or Friday, January 6. But experts from antivirus companies F−Secure, Websense and MessageLabs all agreed on Wednesday, January 4, that this Sober attack is unlikely to cause many problems, because systems administrators and antivirus companies have had time to prepare for it. F−Secure raised the possibility that there might not even be an attack, as Internet service providers could block access to the malicious Websites. Websense agreed that the Sober attack likely won't have a major effect. The worm time bomb is contained in a variant of Sober that hit systems in November, clogging e−mail servers and stalling messages sent to Microsoft's Hotmail and MSN e−mail services.
Source: http://news.com.com/Experts+Sober+time+bombs+under+control/2100−7349_3−6018012.html?tag=cd.top

29. *January 04, IDG News Service* — **Attempts to exploit WMF vulnerability by instant messaging multiply.** Security researchers have logged more than 70 variations of instant messages (IM) attempting to exploit the Windows Metafile (WMF) vulnerability since the first were reported on Saturday, December 31. Malicious WMF files can be distributed via a number of channels, including e−mail, Websites, peer−to−peer file sharing services and IM systems. An attacker may be able to gain control of an IM user's computer by sending such a file, or a link to a Website where one is hosted, through an IM system and then tricking the recipient into clicking on the file or link. The first attempts to do this were logged on Saturday morning, when security researchers at Kaspersky Labs Ltd. received reports of a wave of attacks on Dutch users of the MSN Messenger service. They had received messages inviting them to click on a link to a Website containing an image with the name "xmas−2006 FUNNY.jpg." Anyone following the link would set in motion a chain of events, beginning with the download of a Trojan horse identified by Kaspersky as Trojan−Downloader.VBS.Psyme.br. This in turn would try to install a bot named Backdoor.Win32.SdBot.gen, which would then receive instructions over an Internet Relay Chat (IRC) channel to download IM−Worm.Win32.Kelvir.
Source: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,107455,00.html

30. *January 03, Hackers Center* — **Cisco secure access control server downloadable IP.** A vulnerability in Cisco Secure ACS (Access Control Server), which potentially can be exploited by malicious people to bypass certain security restrictions. The vulnerability is caused due to a design error in the Downloadable IP ACL (Access Control List) feature. This can be exploited by malicious people who know the name of a Downloadable IP ACL configured on the ACS server to authenticate to the RAS/NAS (Remote Access Server/Network Access Server) by using the name of that ACL as their user name. Solution: The vulnerability has been fixed in the following versions: Cisco Secure ACS Version 4.0.1, PIX version 6.3(5), PIX/ASA 7.0(2), Cisco IOS Software Version 12.3(8)T4, and VPN 3000 versions 4.0.5.B and 4.1.5.B.
Source: http://www.hackerscenter.com/archive/view.asp?id=21516

31. *January 03, eWeek* — **Microsoft: Beware of third−party WMF patch.** Microsoft Corp. has slapped a "buyer beware" tag on a third−party patch for the zero−day Windows Metafile (WMF) flaw and promised that its own properly tested update will almost certainly ship Tuesday, January 10. The company's latest guidance comes days after an unofficial hotfix from reverse−engineering guru Ilfak Guilfanov got rare blessings from experts at the SANS ISC

(Internet Storm Center) and anti−virus vendor F−Secure Corp. Guilfanov, author of the IDA (Interactive Disassembler Pro), released an executable that revokes the "SETABORT" escape sequence that is the crux of the problem. The hotfix was tested and approved for use by many security experts, but Microsoft says it cannot vouch for the quality of the fix. Microsoft said its own patch has already been developed and is going through a rigid round of quality assurance testing. Last−minute glitches in the patch testing process could still delay the update. As a general rule, the company never recommends third−party updates. Ever since attackers started exploiting the bug to push malware on vulnerable Windows systems (XP SP2 included), the company has thrown all its security resources into the investigation and patch−creation process, making it virtually impossible to validate the third−party code.
Source: http://www.eweek.com/article2/0,1895,1907562,00.asp

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 functionality that could allow the latest Sober mass mailing worm variants known as "W32/Sober.X", "W32/Sober.Y", and "W32/Sober.Z" to automatically update themselves. These Sober worm variants are dual language (English and German) mass−mailing worms that utilize a built−in SMTP engine to propagate.

There have been over 20 Sober worm variants since October 2003. The latest Sober worm variant has been propagating since November 15, 2005 and will attempt to update itself on January 6, 2006.

The latest Sober worm variant may have a global impact due to its use of pseudorandom URLs that are hosted on servers in European countries, such as Germany and Austria. Systems that have already been compromised by the W32/Sober.X, W32/Sober.Y or W32/Sober.Z worm are expected to receive this update. Once the update is received, the Sober worm variant may execute code that reduces the security protection of infected systems.

US−CERT strongly recommends that users and administrators implement the following general protection measures:

Install anti−virus software, and keep its virus signature files up to date

Do not follow unsolicited web links or execute attachments received in email messages, even if sent by a known and trusted source

Keep up to date on patches and fixes for your operating system

Please refer to Microsoft's Security Advisory at URL: http://www.microsoft.com/technet/security/advisory/912920.ms px

Please visit US−CERT Computer Virus Resources for additional information at URL: http://www.us−cert.gov/other_sources/viruses.html

Exploit for Vulnerability in Microsoft Windows Metafile Handling US−CERT is aware of active exploitation of a vulnerability in how Microsoft Windows handles Windows Metafiles (".wmf"). Several variations of the WMF exploit file have been released that attempt to avoid detection by anti−virus software and intrusion detection and intrusion prevention systems. For more information please review:

Technical Cyber Security Alert TA05−362A / Microsoft Windows Metafile Handling Buffer Overflow: http://www.us−cert.gov/cas/techalerts/TA05−362A.html

US−CERT Vulnerability Note VU#181038 / Microsoft Windows Metafile handler SETABORTPROC GDI Escape vulnerability: http://www.kb.cert.org/vuls/id/181038

Microsoft Security Advisory 912840 / Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution http://www.microsoft.com/technet/security/advisory/912840.ms px

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 25 (smtp), 445 (microsoft−ds), 135 (epmap), 139 (netbios−ssn), 80 (www), 6346 (gnutella−svc), 1434 (ms−sql−m), 32801 (−−−), 27015 (halflife) 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

Nothing to report.
[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