Department of Homeland Security Daily Open Source Infrastructure Report for 13 January 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Daily Times reports in a new twist on a classic "phishing" scam where instead of sending e−mails, hackers took advantage of a recently discovered security hole in Microsoft software and accessed Tennessee−based Y−12 Federal Credit Union's Website and stole $70,000. (See item 8)

- Reuters reports researchers say genetic tests of samples taken from Turkish victims of the bird flu virus show it has made a small change, but probably not enough to make it more dangerous yet. (See item 28)

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 13, Utility Automation & Engineering* — **Nuclear Regulatory Commission considers changes to regulations on products containing radioactive material.** The Nuclear Regulatory Commission (NRC) is considering amending its regulations to improve, update, and clarify its requirements for the possession and use of products containing radioactive material. The NRC says the changes would better ensure future protection of public health and safety, make licensing more effective and efficient, and reduce unnecessary regulatory burden. In addition to changes for exempt distribution licenses, the NRC proposes to make two changes to

the requirements involving general licenses. A general license grants authority to a person for certain activities involving nuclear material and is effective without the filing of an application with the NRC or the issuance of a license to a particular person. Under the proposed changes, general licensees with devices containing certain types and amounts of radioactive material would no longer have to notify the NRC immediately in case of a loss or theft. However, they would have to notify the NRC within 30 days, unless the device has been recovered. The devices covered by this change present limited risk. The proposed changes would also clarify the steps general licensees must take if they wish to transfer a product to a specifically licensed status.
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=245450&p=22

2. *January 12, Miami Herald (FL)* — **Florida utilities defend post−Wilma procedures.** Florida's electric utility companies, including Florida Power & Light (FPL), on Wednesday, January 11, defended their performance during last year's brutal hurricane season, saying they were prepared for the damage and that they responded quickly to restoring power. Geisha Williams, an FPL vice president, said the company's overhead utility power lines fared well during Hurricane Wilma, even though the storm plunged most of South Florida into the dark. She said there is no proof that concrete power poles would have fared better than wooden ones. But the utility did take samples from 1,700 out of 11,000 poles that came down during Wilma in an effort to study what may have happened, so that FPL can determine how to prevent future outages. Preliminary results show that poles were snapped by high winds, regardless of the age or type of pole. Senator Alex Diaz de la Portilla (R), predicted that state legislators may mandate that electric utilities do a better job at inspecting and maintaining overhead power lines. Utility officials said that underground powerlines would be costly and take just as long to fix when damaged, noting that underground lines in coastal communities are subject to flooding from salt water.
Source: http://www.miami.com/mld/miamiherald/13604932.htm

3. *January 12, Reuters* — **U.S. opens Alaskan area to oil leases.** The U.S. government paved the way on Wednesday, January 10, for oil drilling in an Alaskan region three weeks after Congress blocked energy development in the nearby Arctic National Wildlife Refuge. The Interior Department gave final approval to develop the Teshekpuk Lake region, setting up an oil−lease sale in September. The decision came a year after the Bureau of Land Management recommended drilling in the region, which lies west of the wildlife refuge on Alaska's North Slope. The Arctic wildlife refuge (ANWR) is 19.6 million acres, about 50 times larger than the Teshekpuk Lake region. The U.S. Senate last month blocked attempts to open ANWR to drilling. The Bureau of Land Management recommended drilling near Lake Teshekpuk a year ago and says there are about 1.5 billion barrels of recoverable oil. If an oil lease sale is held next September, it could lead to oil drilling as soon as the winter of 2007−08. Lake Teshekpuk and adjacent land is not part of a wildlife refuge and does not need Congressional approval for oil development. Leasing will be subject to a series of new restrictions.
Source: http://thestaronline.com/news/story.asp?file=/2006/1/12/worl dupdates/2006−01−12T131549Z_01_NOOTR_RTRJONC_0_−231605−1&sec =Worldupdates

4. *January 11, Financial Times* — **OPEC nations set for record oil revenues.** The oil revenues of the Organization of the Petroleum Exporting Countries (OPEC), will increase by 10 percent to a record $522 billion this year, the U.S. Department of Energy forecasts. OPEC’s increased

wealth was driven by continuing high oil prices and an increase this year in production. Everything from mergers and acquisitions to the energy sector and art market are expected to benefit. OPEC's 2006 revenue would be the largest in real terms in 25 years. "OPEC countries are undertaking ambitious projects, like weapons purchases by Saudi Arabia," said Manouchehr Takin, senior analyst at the Centre for Global Energy Studies. "It's just been a phenomenal transfer of wealth from consuming to producing nations," said Francisco Blanch, analyst at Merrill Lynch. Forecasts for the average price of New York benchmark crude oil futures in 2006 range between $45 and $75 a barrel, a similar level to that used to calculate total revenue OPEC may expect in 2006. The wildcards are factors such as hurricanes and political unrest.
Source: http://news.ft.com/cms/s/e35bb7ae−82d3−11da−ac1f−0000779e234 0.html

5. *January 11, CBC News (Canada)* — **Oilsands world's largest source of new crude oil by 2010.** Canada's oilsands will become the most important source of new oil in the world by 2010, as conventional crude supplies dry up, CIBC World Markets says in its monthly report. Jeff Rubin, chief economist at CIBC World Markets, said that conventional oil production around the world apparently peaked in 2004. Rubin found total world oil supplies grew by less than one million barrels a day last year. None of that growth came from outside the Organization of the Petroleum Exporting Countries sphere. That finding was particularly surprising because oil prices have doubled in recent years, making exploration of many new areas economically feasible for the first time. Rubin looked at 164 upcoming oilfields in his study and found that new oil is, in fact, being discovered and coming online. Rubin expects a net gain in oil production in coming years, but it will be small and getting smaller. He expects 1.5 million barrels of new oil in 2006 and 2007, but less than a million barrels a day in 2008. Energy companies are finding new oil, but most of it will come from non−conventional sources. Ocean oilrigs are the primary source of new oil today.
Source: http://www.cbc.ca/calgary/story/ca−oilsands−crude20060111.ht ml

6. *January 10, Las Vegas Review−Journal (NV)* — **First direct transmission link between Northern and Southern Nevada electric utilities planned.** Sierra Pacific Resources on Monday, January 9, announced plans for the first direct transmission link between its Northern and Southern Nevada electric utilities, a line that would carry power from a new coal−fired power plant complex near Ely, NV. The Ely Energy Center would be the biggest energy project in Nevada since the construction of the Hoover Dam. "It will also decrease our dependence overall on purchased power and natural gas," said Walt Higgins, chairman and chief executive officer of Sierra Pacific Resources. The first of two 750−megawatt, coal−fired power units would start generating power in the Steptoe Valley near Ely by 2011. Within a few years, the company proposes to complete a second, 750−megawatt plant and two 500− megawatt coal gasification plants. Combined, the four plants could produce up to 2,500 megawatts. The company proposes to build a line from the power plant site in Steptoe Valley north of Ely to the Falcon−Gonder transmission line in Northern Nevada and south to the Harry Allen substation near Las Vegas. The 500−kilovolt line would provide greater reliability to Nevada Power and Sierra Pacific Power, because they could draw power from the other utility in the event of a major outage.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8 knpp%5E%5Bfkrsonv%5BTfc%7D38%7Dbfel%5Dv

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

7. *January 11, Government Computer News* — **SOCOM has higher technology in mind for special ops forces.** Special Operations Command's (SOCOM) forces are on the path of transformation, and that transformation entails improving their technology processes, said Vice Adm. Eric T. Olson, deputy commander of SOCOM. "We've invested heavily in top−notch systems and have reduced our load from five to six radios per person to two to three radios per person," Olson told an audience Wednesday, January 11, at the Armed Forces Communications and Electronics Association's West 2006 show, referring to special operations forces deployed around the world. SOCOM has a rapid acquisition process which has seen equipment for force protection and specialized unmanned aerial vehicle (UAV) sensors fielded in as little as seven days, Olson said. The command has partnered with the Department of Defense's Office of Force Transformation to conceptualize the Stiletto/Wolf ship, a prototype vessel that operates at high speeds and includes an electronic keel that was created for mission reconfiguration and clustered supercomputing and the capability to launch UAVs. Still, Olson told the audience that SOCOM needs more bandwidth to run streaming videos and an ever−growing data flow. Olson said special operations forces are also looking for Web−based collaboration software systems and the capability to conduct audio chats and white−boarding files.
   Source: http://www.gcn.com/vol1_no1/daily−updates/37968−1.html

[Return to top]

Banking and Finance Sector

8. *January 12, Daily Times (TN)* — **Cyber thieves steal $70,000 from credit union in new method of phishing.** In a new twist on a classic "phishing" scam, cyber thieves have pilfered around $70,000 so far from Y−12 Federal Credit Union and its customers. Usually, phishers will send out an e−mail claiming to be from a bank or credit card company and direct the recipient to a phony Website asking for financial information. In the case of Y−12, no e−mails were ever sent. "That's the new wrinkle in this case," Y−12 Federal Credit Union spokeperson Chris Smith. Instead of sending e−mails, hackers took advantage of a recently discovered security hole in Microsoft software and accessed Y−12 Federal Credit Union's Website. For around 90 minutes Monday evening, January 9, when customers would enter their user name and password into the legitimate site, they were then redirected to a bogus site −− based in Greece, Smith said −− that asked for their credit card number and personal identification number or PIN. The hackers then used the information to create magnetic strips like those found on the back of credit and ATM cards. The credit union and the Federal Bureau of Investigation have spotted ATM transactions related to the Y−12 breach all across the United States and even as far away as Pakistan.
   Source: http://www.thedailytimes.com/sited/story/html/227429

9. *January 12, Finextra* — **Identity protection survey released.** A survey of 28 financial firms that analyzed consumer−facing online identity fraud prevention, detection, and resolution capabilities has been released by Javelin Strategy & Research. Javelin used a combination of online review and direct mystery−shopper research to score banks on a 100−point scale that included 28 consumer−facing capabilities that could be implemented. None of the surveyed banks allow users to limit or prohibit international or online transactions in order to increase security. Furthermore, while banks have significantly improved their customer education capabilities, Javelin says most firms have yet to implement stronger authentication. The study also revealed that the majority of banks do not offer customer−driven alerts regarding changes to personal information, balance transfers, and unusual account activity, while none of the banks surveyed offer e−mail alerts of changes to credit bureau information −− an important indicator of new account identity fraud.
Survey: http://www.javelinstrategy.com/reports/
Source: http://finextra.com/fullstory.asp?id=14747

10. *January 11, MarketWatch* — **U.S. identifies money−laundering threats.** U.S. financial and law enforcement agencies on Wednesday, January 11, identified threats to banks, insurance companies, and other financial institutions from money laundering. In a report written by 16 government agencies, officials said that regulators and law enforcement are improving their anti−money−laundering efforts. "The volume of dirty money circulating through the U.S. is undeniably vast and criminals are enjoying new advantages with globalization and the advent of new financial services such as stored−value cards and online payment systems," the report said. The report highlighted moves by U.S. customs officials to combat bulk cash smuggling and underscored the increase in Drug Enforcement Administration anti−money−laundering resources and the Internal Revenue Service's new office for combating fraud. U.S. authorities are concerned banks and other financial institutions could be used for money laundering activities including hiding embezzled public funds and concealing money linked to terrorist organizations. Banks are at risk from illegal activity conducted by cross−border wire transfers and a failure to catch criminals at private banks. Federal Reserve Governor Susan Bies said the report is the beginning of better communication between government and financial companies. "We think this is the beginning of much more information flowing," she said.
Source: http://www.marketwatch.com/news/story.asp?guid=%7B5E837F13%2DEC75%2D4977%2DBF8F%2D767864D9DAB7%7D&dist=rss&siteid=mktw

11. *January 11, The Business Review (NY)* — **Scammers phish for Chase Bank customers.** New York's Consumer Protection Board (CPB) is warning Chase Bank customers to watch out for "phishing" computer scams. In this case the phishers are sending e−mails to consumers in which they claim to represent Chase Bank. The e−mail warns the reader that someone has tried to access their bank account from a foreign Internet address and instructs them to correct the situation by clicking on a Website link in the e−mail. Doing so will allow the scam artists to obtain information on that person. Legitimate banks, Ebay and other legitimate online services do not send out these kinds of e−mail messages said Teresa A. Santiago, Chairperson and Executive Director of the CPB.
Source: http://www.bizjournals.com/albany/stories/2006/01/09/daily33 .html?from_rss=1

12.

January 11, IDG News Service — **Bank tape lost with data on 90,000 customers.** A computer tape from a Connecticut bank containing personal data on 90,000 customers was lost in transit recently, the bank reported on Wednesday, January 11. People's Bank, based in Bridgeport, CT, said the tape contains names, addresses, Social Security numbers, and checking account numbers. It was bound for the TransUnion LLC credit−reporting bureau, based in Woodlyn, PA, via UPS, the bank said. UPS is investigating the incident, said UPS spokesperson Heather Robinson. The bank has not received any reports of unauthorized activity on the affected accounts and has no reason to believe the data has been improperly used, according to People's statement. The bank considers misuse of the data "highly unlikely." UPS also has no evidence that the package was compromised or stolen, according to Robinson. There isn't enough information on the People's Bank tape to allow anyone to get into a customer's account, according to the bank. It does not contain checking account balances, debit card numbers, personal identification numbers, or birth dates. In addition, the tape can't be read without a mainframe and software, according to the bank. The data on the tape involves customers that have a People's Bank personal credit line.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,107661,00.html

13. *January 11, ZDNet (Australia)* — **Windows flaw allows new type of phishing.** In an evolution of the phishing phenomenon, cyber−criminals are using the recently patched Windows WMF vulnerability to hook victims without needing the user to visit a bogus Website. The WMF vulnerability that affects all versions of Windows could provide phishers with an unwelcome tool, according to Dan Hubbard, senior director at security firm Websense. The WMF exploit is already being used by phishers because it provides them with a way of stealing banking details without having to first trick the victim into giving up their details. "Now by simply visiting a Website −− it doesn't even have to be a bank Website −− they drop a keylogger onto your machine and use the vulnerability that may not be fixed," said Hubbard. Financial institutions have spent years educating their customers to avoid suspicious e−mails, but phishing has moved on. "The problem is not decreasing, it is changing. [The banks] are correct that people are getting wise to clicking on e−mail links...But cybercriminals have realized that there is a lot of money to be made and are shifting the way they gather information from end users by using vulnerabilities to install keyloggers and screen scrapers."
Source: http://www.zdnet.com.au/news/security/soa/Windows_flaw_allows_phishing_without_a_hook/0,2000061744,39232189,00.htm

[Return to top]

Transportation and Border Security Sector

14. *January 12, Philadelphia Inquirer* — **Massive New Jersey port project proposed.** New Jersey officials on Wednesday, January 11, touted a $5 billion waterfront development plan as an alternative to deepening the Delaware River's shipping channel and said it would spur thousands of jobs, new housing and improved ports. Along with a member of the U.S. House and two New Jersey state senators, the Delaware River Port Authority made public the results of a $600,000 study that seeks to develop 50 miles of New Jersey waterfront, from Pennsauken in Camden County through Gloucester and Salem Counties. The plan would develop a cargo ship facility at a former oil terminal in Paulsboro. And, it would improve and enhance marine facilities in Carneys Point, Gloucester City, Greenwich Township, and the ports at Camden's

Broadway and Beckett Street terminals. The plan, which officials say would be financed with public and private money, comes as the two states are deeply divided over whether to dredge the shipping channel from 40 to 45 feet. The dispute centers on New Jersey officials' contention that dredging is a waste of money and threatens water quality and river wildlife, while Pennsylvania officials argue that it is the only way to keep Delaware River ports competitive.
Source: http://www.philly.com/mld/inquirer/13604825.htm

15. *January 12, Aero−News Network* — **FAA rules employees at outsourced facilities must undergo drug testing.** The Federal Aviation Administration (FAA) ruled Wednesday, January 11, that, effective April 10, all employees at outsourced repair and maintenance facilities in the U.S. must undergo the same drug and alcohol testing procedures as those directly employed by domestic airlines. The move was met with approval by the Aircraft Mechanics Fraternal Association (AMFA), but union representatives also say more must be done. On Thursday, January 12, AMFA called on the FAA to close another safety gap, by extending the testing program to cover repair shops outside of the U.S. as well. "In the post−9/11 era, it's shocking that the planes Americans fly on are increasingly being worked on by individuals whose backgrounds have never been checked, and who have not been tested for drug and alcohol abuse," said AMFA National Director O.V. Delle−Femine.
Source: http://www.aero−news.net/index.cfm?ContentBlockID=2fbdc6d3−501f−4019−9d41−8c72bc9ccbaf

16. *January 12, Associated Press* — **Rain causes transportation problems for the Northwest.** Heavy rain triggered mudslides that halted Amtrak passenger train service between Vancouver, British Columbia, and Portland, OR −− the second disruption in the area in a week. Mudslides also blocked part of a major highway Tuesday, January 10, and chased residents out of a University of Washington fraternity annex, officials said. Passenger rail service was to remain closed for at least 48 hours, said Gus Melonas, a spokesperson for Burlington Northern Santa Fe Corp., which owns and operates the tracks. Mudslides on Friday, January 6, knocked out service to both Amtrak and commuter trains. Buses carried Amtrak passengers around blockages and replaced commuter trains between Seattle and Everett, WA.
Source: http://www.kstp.com/article/stories/S13372.html?cat=1

17. *January 12, Associated Press* — **Woman scuffles with flight attendants, passengers.** A woman scuffled with flight attendants and another passenger on a United Express flight Wednesday, January 11, and then claimed a bomb was on board after the plane was diverted, authorities said. No bomb was found aboard the aircraft, which left Eugene, OR, for Denver but was diverted to Salt Lake City, authorities said. The woman was charged with interference with a flight crew. Bogdana Georgieva, 35, of Bulgaria, threw a passenger into the aisle, began yelling, tried to remove her shirt, and threw items at other passengers, court documents said. The pilot diverted the plane to Salt Lake City. During landing, Georgieva ran toward the cockpit and was stopped by flight attendants, with whom she got in another scuffle, documents said. Passengers subdued her. The plane was evacuated and checked for explosives. Passengers were allowed back, and the flight continued to Denver, said FBI agent Patrick J. Kiernan. Georgieva was sent to a Salt Lake City hospital for evaluation.
Source: http://www.cnn.com/2006/TRAVEL/01/12/flight.disturbance.ap/i ndex.html

18.

January 11, GovExec — **Coast Guard modernization program could move faster, contractor says.** The Coast Guard's long−term modernization program known as Deepwater could be dramatically accelerated from the current 25−year schedule if adequate funding is provided, contract officials said earlier this week. The program, aimed at upgrading aging equipment used more than 50 miles offshore, has drawn criticism almost since its inception in the late 1990s, for its lengthy time frame and unwieldy budget. "We would welcome an acceleration, and it would achieve more economical production rates," said Leo Mackay, president of Integrated Coast Guard Systems (ICGS), during a presentation to the press on Monday. One of the program's key accomplishments so far has been the 11−year acceleration of plans to develop a fast response cutter, a multipurpose vessel designed to replace the Coast Guard's aging 110−foot patrol boats, Mackay said. The Coast Guard awarded the initial Deepwater contract based on pre−9/11 needs assessments, and has since seen a significant increase in counterterrorism responsibilities. An April 2004 report by the RAND Corp., a nonpartisan research organization based in Santa Monica, CA, concluded that an acceleration of the program, combined with the purchase of more assets, would help the Coast Guard meet this expanded mission.
Source: http://www.govexec.com/story_page.cfm?articleid=33149&dcn=to daysnews

19. *January 11, Associated Press* — **Pilots warned of Alaskan volcano eruption.** A volcano on an uninhabited island erupted early Wednesday, January 11, spewing ash about five miles into the sky and prompting air traffic authorities to warn planes to steer clear of the cloud. The ash from Augustine Volcano was not expected to reach Anchorage, Alaska's most populous city nearly 200 miles to the northeast, meteorologists said. Flights were restricted temporarily in a five−mile radius around the volcano and for 50,000 feet above it, said Federal Aviation Administration spokesperson Mike Fergus. The ash can clog jet engines. Cargo or passenger traffic from Asia usually fly through the area to Anchorage but could be easily rerouted, Fergus said. "It's not posing any significant traffic problems," he said. Two explosions earlier in the day indicated an eruption at the volcano, said geologist Jennifer Adleman of the Alaska Volcano Observatory. The 4,134−foot volcano last erupted in 1986. Ash from a seven−mile−high column drifted over Anchorage and forced flights to avoid the skies over Cook Inlet.
Source: http://www.cnn.com/2006/TECH/science/01/11/alaska.volcano.ap /index.html

[Return to top]

Postal and Shipping Sector

20. *January 12, Federal Times* — **High fuel costs spur Postal Service conservation.** Faced with unexpectedly high fuel costs this year, the U.S. Postal Service has been ramping up savings measures, hoping to cut hundreds of millions of dollars from energy bills over the next decade. In the last fiscal year that ended September 30, the additional cost to the agency resulting from the summer energy crisis and the post−Katrina natural gas shortage totaled about $400 million, according to Michael Fanning, Postal Service program manager for energy management. "Energy is the third−largest cost center in the Postal Service, following salaries and benefits, and automation," Fanning said. High energy costs will likely continue into the new year and beyond and the Postal Service must take steps on many fronts to cut energy use where it can and get the most of its fuel where it can't, Fanning said. One significant energy−saving move

could come after a suppliers' conference January 13 at Postal Service headquarters in Washington, at which the agency will explain to prospective contractors its desire to award Shared Energy Savings contracts. Under these deals, contractors outfit postal facilities to be more energy efficient −− such as with renewable energy, geo−thermal heat pumps, photovoltaic energy sources and micro−turbine wind power.
Source: http://federaltimes.com/index2.php?S=1452397

[Return to top]

Agriculture Sector

21. *January 12, Associated Press* — **U.S. Department of Agriculture pulls funding for citrus canker fight.** In a major setback to Florida's battle against citrus canker, the U.S. Department of Agriculture (USDA) argued that the fight is hopeless and pulled its funding for current eradication efforts. "The disease is now so widely distributed that eradication is infeasible," USDA deputy secretary Chuck Conner wrote in a letter received Wednesday, January 11, by Florida Agriculture Commissioner Charles Bronson. Conner said the hurricane seasons of 2004 and 2005 spread the disease too much to make it eradicable and a new management plan must be devised. Federal support amounted to more than $36 million so far this year. Federal money will no longer fund tree removal, the basis of the canker eradication program. Canker causes fruit and leaves to drop prematurely. Canker also creates unsightly lesions on fruit, making it harder to sell. The disease itself doesn't kill the tree.
Source: http://www.theledger.com/apps/pbcs.dll/article?AID=/20060112 /APF/601120591

22. *January 12, Globe and Mail (Canada)* — **Stowing seeds to survive a disaster.** The future of humankind may soon be buried deep within a sandstone mountain, locked in permafrost, and encased in concrete behind blast−proof doors designed to foil terrorists. The experiment to preserve two million seeds, representing a veritable Noah's ark of the world's food crops, is expected to take shape this year on a remote Norwegian island. The seed bank, sponsored by the Norwegian government and a private trust promoting crop diversity, is meant to preserve the genetic building blocks of edible plants in the case of nuclear war, crop disease, catastrophic climate change, earthquakes or other natural or man−made disasters. "If the worst came to the worst, this would allow the world to reconstruct agriculture on this planet," said Cary Fowler, executive secretary of the Global Crop Diversity Trust in Rome. The trust was established in association with the United Nations Food and Agricultural Organization and aims to collect and safeguard crop diversity. The Norwegian cold storage vault, should eventually stock seeds from plant varieties from every continent. Most of the seeds will be taken from inventories in existing seed banks in Africa, Asia, and Latin America, where the safety of the storehouses has been compromised by electricity failures, political turmoil, and poor security.
Source: http://www.theglobeandmail.com/servlet/story/RTGAM.20060112.wxseeds12/BNStory/International/

23. *January 11, Associated Press* — **Park Service captures some Yellowstone bison for slaughter.** About 160 wandering bison have been captured at Yellowstone National Park, and officials there plan to send the animals straight to slaughter, without first testing them for the disease brucellosis, a park spokesperson said Wednesday, January 11. Al Nash also said as many as 200 bison could be captured near the park's northern boundary by day's end. Nash said

the bison, some of which were on private property, had been hazed −− in some cases, repeatedly. The park said in a news release that hazing was no longer a safe or effective option for dealing with bison in the area. Many of the park's bison have brucellosis, as do some elk in the region, and the disease can cause cows to abort. Under a state−federal management plan, aimed at reducing the potential spread of brucellosis from bison to cattle in Montana, wandering bison can be hazed, or captured and tested for the disease. Bison that test positive are shipped to slaughter. But given the size of Yellowstone's bison herd, officials have the option of sending captured bison straight to slaughter, without testing them.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednew s/2006/01/11/build/state/28−bison.inc

[Return to top]

Food Sector

24. *January 11, Animal and Plant Health Inspection Service* — **Philippine market opened to live U.S. breeder cattle.** The Philippines Department of Agriculture recently agreed to allow live U.S. breeder cattle imports into the country under the terms and conditions of the Philippines Import Health Protocol for Live Cattle from the U.S. Importers are required to obtain a veterinary quarantine clearance from the Philippine Department of Agriculture's Bureau of Animal Industry prior to the shipment of animals. Specific import terms and conditions for the import of live breeder cattle are outlined in the health protocol.
Source: http://www.aphis.usda.gov/newsroom/content/2006/01/philcat.s html

[Return to top]

Water Sector

25. *January 12, Associated Press* — **Teflon chemical found in spring water.** Bottled water provided to Ohioans whose tap water contained C8 −− a chemical used to make Teflon has tested positive for the same chemical. The bottled water will be provided until filters are installed at the Little Hocking Water Association, in Washington, OH. Tests have shown that customers in that district had 80 times more C8 in the blood than the general population. More than 1,000 residents in the district received bottled water from Crystal Spring Water. When Little Hocking officials decided to test the bottled water to assess the accuracy of C8 testing methods, they found traces of the chemical in the Crystal Spring bottles. Crystal Spring owner Gary Matheny said he conducted two tests after hearing of the results and found C8 as well. Matheny said the company has started giving residents treated water and is installing a filter to remove C8 from the spring water the company uses. The bottled water showed C8 levels at 13 to 17 parts per trillion (ppt). The well supply that provides the residents' tap water contained 3,500 ppt to 7,200 ppt.
Source: http://www.cbsnews.com/stories/2006/01/12/health/main1203422 .shtml

[Return to top]

Public Health Sector

26. *January 12, New Kerala (India)* — **Uttar Pradesh to launch drive against polio.** Uttar Pradesh, which has the distinction of housing about one third of total polio cases in India, will go for a decisive eight−phase pulse polio immunization program in 2006, starting January 15. The state, along with Bihar, has reported most of the polio cases, notwithstanding an aggressive countrywide pulse polio campaign launched about a decade ago. The year 2006 would see Uttar Pradesh go all out against polio with a resolve to uproot the health menace from the state. State Family Welfare Minister Ahmad Hassan said. As per official statistics, Uttar Pradesh, the most populous state in India, reported 28 polio cases out of a total of 63 cases in the country in 2005.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.newkerala.com/news.php?action=fullnews&id=84920

27. *January 12, International Herald Tribune* — **Europe increases its efforts to stop bird flu.** As Turkish officials shifted into high gear to control the outbreaks of avian influenza that have spread across their country, neighboring countries and nations across the European Union enhanced their surveillance efforts so the virus would be detected quickly if it crossed the border. Officials with the Food and Agriculture Organization (FAO) have expressed worries that the outbreaks in Turkey are so widespread that it may now be impossible to eradicate the H5N1 virus. If Turkish measures are unsuccessful and the virus become endemic in Turkey −− as it is in parts of southeast Asia −− that would create a constant reservoir of the disease at the edge of Europe. The FAO urged countries near Turkey to maintain a "high alert" for the virus and to inform the public about the need to report all sick birds and to warn about the dangers of contact. The organization specifically mentioned Armenia, Azerbaijan, Georgia, Iraq, Iran, and Syria. More worrisome, it is possible that avian influenza is already present in at least some of these neighboring countries, officials said. The European Commission announced that it was upgrading its surveillance requirements for all member states, which must submit proposals for national early detection programs by February 7.
Source: http://www.nytimes.com/2006/01/12/international/europe/12cnd −flu.html

28. *January 12, Reuters* — **Tests show bird flu virus is evolving as expected.** Genetic tests of samples taken from Turkish victims of the bird flu virus show it has made a small change, but probably not enough to make it more dangerous yet, researchers said on Thursday, January 12. H5N1 avian influenza has caused a burst of human infections in Turkey and has been found in flocks of poultry across the country. It has killed at least two children in Turkey, probably three, and infected a total of 18 people, according to Turkish authorities. Globally it has infected 147 people and killed 78 of them, according to the World Health Organization (WHO), which only includes four of the Turkish cases. Scientists are carefully watching the virus to see if it makes the changes needed to allow it to easily pass from human to human. There were two different strains of virus in the bodies of the teenage victims, said Ruben Donis, team leader of the molecular genetics team of the U.S. Centers for Disease Control and Prevention's Influenza branch. "One was a regular virus like we have seen in poultry in Turkey before," Donis said. But half the viruses had a mutation in a protein called hemagglutinin, which influenza viruses use to attach to the cells they infect.
Source: http://news.yahoo.com/s/nm/20060112/hl_nm/birdflu_mutation_d c

29. *January 12, Associated Press* — **Health dangers, travel studied.** Visitors to exotic locales have long been warned not to drink the water. But tourists also face plenty of other health

dangers −− including food, mosquitoes and bugs on the ground. The records of ill travelers treated at a network of 30 travel−medicine clinics on six continents, called GeoSentinel, have yielded the most comprehensive picture yet of the illnesses most likely to strike visitors to particular regions of the Third World. "This is a real blueprint" for doctors, said David Freedman, lead researcher of a study. "Where the traveler has returned from really determines what diagnoses you should worry about and what you should test for." Each year, about eight percent of the more than 50 million travelers to developing countries become sick enough to seek health care during their trip or when they return home. And foreign travel, including business trips and immigrants' visits back home, is on the rise, with more than 760 million people crossing borders in 2004.
Study abstract: http://content.nejm.org/cgi/content/short/354/2/119
Source: http://seattletimes.nwsource.com/html/nationworld/2002734783_travelsick12.html

[Return to top]

Government Sector

30. *January 12, Boston Globe* — **Court to set safe room for victims and witnesses.** Crime victims and prosecution witnesses in Suffolk County, MA, will soon have a room where they can wait before testifying so they can avoid being intimidated by supporters of defendants. The room is an initiative that high−ranking judges and the county's top prosecutor unveiled Thursday, January 12. The "safe haven," as Suffolk District Attorney Daniel F. Conley described it, will be located in an office once used by a former chief justice of the state's Superior Court in the Suffolk Courthouse in Pemberton Square in Boston. The judiciary is providing the office because of rising concerns about witness intimidation that are spurring state legislation to protect witnesses, and new security procedures at courthouses. Thursday's news conference comes two days after the ban on anyone wearing clothing that bears the phrase "Stop Snitching," which authorities said spectators have donned to intimidate witnesses. There are also now strict limits on the use of cell phones in courthouses, citing recent cases in which spectators pointed mobile−phone cameras at witnesses, jurors, or law−enforcement officials.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/01/12/court_to_set_safe_room_for_victims_and_witnesses/

31. *January 12, Purcell Register (OK)* — **Cameras to provide courthouse security.** Tightened security will soon be coming to the McClain County Courthouse in Oklahoma as officials recently received a grant to provide more security for the public’s building. “We will be working very hard to maintain security of the courthouse and at the same time not inconveniencing the public,” McClain County Sheriff Don Hewett said. The security comes after the sheriff’s office was awarded a $25,400 grant. The Critical Infrastructure Protection Grant is federally funded from the Department of Homeland Security. McClain County is one of 15 sheriff’s offices in Oklahoma receiving the grant. Hewett said 11 video surveillance cameras are going to be placed strategically throughout the courthouse. The cameras will be monitored around the clock by sheriff’s office personnel. Another security addition will be that all of the courthouse employees will have an identification badge. Just in case anything was to ever occur, Hewett said the staff would be easily identified through this new additive. The sheriff said the cameras will be inconspicuous, while still offering the protection needed for a public building and the county citizens.

Source: http://www.purcellregister.com/article−display.asp?idnum=242 8

[Return to top]

Emergency Services Sector

32. *January 12, The Digital Collegian (PA)* — **Pennsylvania county upgrades technology.** Cell phone users calling Centre County 911 may soon be able to call in an emergency without having to know their exact location. This spring, Centre County 911 will be upgraded with new technology that allows the emergency center to identify the exact location and identity of the cell phone caller. Centre County 911 Communications Director Dan Tancibok said, "As of now, the call is routed to the nearest cell phone tower with the best signal…we have no way of identifying the caller's exact location, and often the caller cannot tell us where they are." Tancibok said the current system does not give the department a callback number. The update will give the operator the phone number of the cell phone as well as the latitude and longitude of the caller's location.
Source: http://www.collegian.psu.edu/archive/2006/01/01−12−06tdc/01− 12−06dnews−02.asp

33. *January 12, Beaumont Enterprise (TX)* — **Texas leaders bracing for next disaster.** On Wednesday, January 11, local leaders from Beaumont, TX, took what they learned during Hurricane Rita and the weeks and months that followed and worked out a road map to deal with the next disaster. Issues including what went right and wrong, staffing levels for emergency operations centers, communications, body storage for the dead, shelters and evacuation were on the table at a meeting at the Ford Park Exhibit Hall. Jefferson County Judge Carl Griffith said, "We already have a plan, and this will update our plan…this is lessons learned, and we will incorporate all lessons into the new plan." Vidor Mayor Joe Hopkins said most of the problems his city faced in the wake of the storm revolved around the distribution of scarce resources such as fuel, food and generators. He suggested a single organization be assigned the job of doling out supplies after disasters. "I think it would be great if the state did that, instead of them having to call 200 or 300 different entities," Hopkins said. Like many local leaders, Hopkins said he was unable to get answers when he contacted different agencies in Rita's aftermath.
Source: http://www.southeasttexaslive.com/site/news.cfm?newsid=15913 661&BRD=2287&PAG=461&dept_id=512588&rfi=6

34. *January 11, Hendersonville Star News (TN)* — **Preparing Tennessee county for possible disasters.** Local officials feel certain that Sumner County, TN, is extremely well prepared for a possible disaster, but in order to test this theory, they decided to have their own “table−top” exercise. On Monday, December 12, over 70 professionals took part in this exercise at the Sumner County Emergency Management Agency (SCEMA) Operations Center in Gallatin. Participants included several local officials and representatives from every fire and police department in Sumner County, Tennessee Valley Authority (TVA), Cumberland Electric Membership Corporation, Gallatin Department of Electricity, Nashville Electric Service, the Health Department, local hospitals/medical centers, the Red Cross, Federal Bureau of Investigation, Tennessee Bureau of Investigation, Tennessee Emergency Management Agency, Federal Emergency Management Agency, and Homeland Security. The scenario for the exercise centered on a simulated terrorist attack on the TVA power generation plant in Gallatin. The exercise was designed to improve the understanding of response plans, identify

opportunities or problems with current plans, and develop a cooperative attitude. The objectives were: inter−agency planning and coordination, resource coordination, threat/hazard−related issues, and options in providing timely information to the public and media.
Source: http://www.rctimes.com/apps/pbcs.dll/article?AID=/20060111/MTCN0505/301110061/1320/MTCN0305

35. *January 11, Technology Review* — **Rescue robots can help in hazardous situations.** William L. "Red" Whittaker is director of the Field Robotics Center and founder of the National Robotics Engineering Center at Carnegie Mellon University in Pittsburgh, PA. His expertise includes developing robots for hazardous duty and for performing three−dimensional (3−D) mapping in environments such as coal mines and volcanoes. Soon after a near−fatal mine disaster at Quecreek, PA, in mid−2002, interest grew in his center's subterranean robotics and its mapping capabilities. A prototype machine they'd built was sent into an abandoned coal mine near Pittsburgh created accurate 3−D maps of its surroundings. Technology Review asked Whittaker to discuss the possible role of robots in aiding and rescuing miners. Whittaker states, “First, it's important to realize that robots are not yet deployed as standard tools in mine rescue today. Rescue robots in the future will certainly enter mines −− under the unknown conditions of dust and gas and inundation and roof fall −− and will be crucial for exploring and characterizing conditions and reporting back to command centers. Once robots have the capability to get in around, they could also provide communications and visual and map sensing, deliver objects to aid trapped people, and detect vital life signs.
Source: http://www.technologyreview.com/NanoTech/wtr_16136,303,p1.ht ml

36. *January 11, Herald News (NJ)* — **New Jersey county plans to upgrade communications network for first responders.** Passaic County, NJ, plans to spend a $1.9 million Department of Homeland Security grant on a communications network that would link the county's main law enforcement offices, emergency units, and colleges, said County Prosecutor James Avigliano. "It would be instant communication between all the people throughout the county involved in Homeland Security," said Avigliano. The network would be used on a daily basis, as well as in emergency situations, he said. Avigliano expects the fiber−optic network to be working by September, 2006. It would connect down−county municipal police and fire departments with the Sheriff's Department, the Intelligence Unit of the Prosecutor's Office, and security units at Montclair State and William Paterson universities, he said. The network is part of Avigliano's plan to modernize the county's law enforcement and emergency communications infrastructure by providing what is known as interoperability between various first−response services.
Source: http://www.bergen.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXk2MDYmZmdiZWw3Zjd2cWVlRUV5eTY4NTYwNjcmeXJpcnk3ZjcxN2Y3dnFlZUVFeXkz

[Return to top]

Information Technology and Telecommunications Sector

37. *January 12, Security Focus* — **Linux Kernel NAT handling memory corruption denial of service vulnerability.** Linux Kernel is reported prone to a denial of service vulnerability. Due to a design error in the kernel an attacker can cause a memory corruption, ultimately crashing the kernel, denying service to legitimate users. Solution: The vendor has released versions

2.6.13 and 2.4.32−rc1 of the kernel to address this issue.
For more solution details: http://www.securityfocus.com/bid/15531/solution
Source: http://www.securityfocus.com/bid/15531/references

38. *January 11, Hackers Center* — **Symantec Norton protected recycle bin security bypass vulnerability.** A vulnerability has been identified in Norton SystemWorks, which could be exploited by local attackers or malware to hide certain information. This is due to an error in the "NProtect" directory of the Norton Protected Recycle Bin that is hidden from the Windows FindFirst/FindNext APIs, which could cause malicious files in the "NProtect" directory to not be scanned during scheduled or manual virus scans.
Source: http://www.hackerscenter.com/archive/view.asp?id=21809

39. *January 11, Hackers Center* — **Microsoft Visual Studio "UserControl.Load" code execution vulnerability.** A vulnerability has been identified in Microsoft Visual Studio, which could be exploited by attackers to execute arbitrary commands. This is due to a design error where a code passed to the "UserControl.Load" event of a control is automatically executed when opening a project containing a specially crafted form, which could be exploited by attackers to execute arbitrary commands by convincing a user to open a solution file in a malicious Visual Studio project.
Source: http://www.hackerscenter.com/archive/view.asp?id=21807

40. *January 11, Channel Register (United Kingdom)* — **European IT spending shrinking.** IT spending across Europe is under even more pressure and budgets will grow by just 1.6 percent in 2006, compared to 2.9 percent last year. Researchers from Forrester found that more than half of European firms plan to reduce IT budgets this year. The main priority across Europe is for spending on security, anti−virus and host intrusion detection. For IT services price pressure is the main concern, with nearly half of European firms saying that cutting costs is an important or critical priority for the year ahead. Miguel Angel Mendez, associate analyst at Forrester Research, said the caution on IT spending was at odds with people's more optimistic view of their own industries −− 60 percent of respondents expect the coming year to be good or okay for their industries. The feeling in the United Kingdom seems slightly more optimistic −− British firms expect to increase IT spending by 2.3 percent, but only 20 percent of this will go on new developments. Big technology brands such as Cisco, HP, IBM, Microsoft, SAP and Oracle get the lion's share of purchasing preferences.
Source: http://www.channelregister.co.uk/2006/01/11/it_spending_shri nks/

41. *January 11, Search Security* — **Federal Bureau of Investigation says attacks succeeding despite security investments.** Despite investing in a variety of security technologies, enterprises continue to suffer network attacks at the hands of malware writers and inside operatives, according to an annual Federal Bureau of Investigation (FBI) report released Wednesday, January 11. The 2005 FBI Computer Crime Survey was taken by 2,066 organizations in Iowa, Nebraska, New York, and Texas late last spring, which survey organizers deemed a good sample of enterprises nationwide. The report is designed to "gain an accurate understanding" of computer security incidents experienced "by the full spectrum of sizes and types of organizations within the United States," the FBI said. The 23−question survey is not the same as the CSI/FBI Computer Crime and Security Survey. The survey addressed such issues as the computer security technologies enterprises used, what kinds of

security incidents they've suffered and what actions they've taken. Among the findings: 1) Security software and hardware failed to prevent more than 5,000 incidents among those surveyed; 2) A common point of frustration came from the nonstop barrage of viruses, Trojans, worms and spyware; 3) Use of antivirus, antispyware, firewalls and antispam software is almost universal among those who responded. But the software apparently did little to stop malicious insiders.
FBI 2005 Computer Crime Survey: http://www.fbi.gov/publications/ccs2005.pdf
Source: http://searchsecurity.techtarget.com/originalContent/0,28914
2,sid14_gci1157706,00.html

42. *January 11, Networking Pipeline* — **Networking's big players form ethernet industry alliance.** Some of the leading players in the network equipment industry have formed a new organization dedicated to promoting Institute of Electrical and Electronics Engineers (IEEE) 802 Ethernet standards. The Ethernet Alliance will support the advancement of existing and emerging Ethernet technologies by providing member companies with the resources to stimulate market acceptance and accelerate the introduction of new networking products. Positioning itself as the "voice" of the Ethernet industry, the alliance will cultivate efforts to define and develop new network technologies based on the IEEE 802 standard, and by providing consumer education on product options. Members include 3Com, ADC, Agere Systems, AMCC, Aquantia, Broadcom, Force10 Networks, Foundry Networks, Intel, Lawrence Berkeley Labs, Pioneer Corporation, Quake Technologies, Samsung, Sun Microsystems, Tehuti Networks, Tyco Electronics, The University of New Hampshire InterOperability Laboratory (UNH−IOL), and Xilinx.
Source: http://nwc.networkingpipeline.com/175803497;jsessionid=JX3A0
DVU2HBO0QSNDBECKH0CJUMEKJVN

43. *January 11, Tech Web* — **Microsoft's newest bug could be serious, researcher says.** The Outlook and Exchange vulnerability disclosed by Microsoft Tuesday, January 10, has the potential to become a much more virulent problem than the long−hyped Windows Metafile (WMF) bug patched last week, said one of the e−mail flaw's discoverers Wednesday, January 11. The TNEF (Transport Neutral Encapsulation Format) vulnerability, which Microsoft spelled out in the MS06−003 security bulletin, is a flaw in how Microsoft's Outlook client and older versions of its Exchange server software decode the TNEF MIME attachment. TNEF is used by Exchange and Outlook when sending and processing messages formatted as Rich Text Format (RTF), one of the formatting choices available to Outlook users. "All that's required to exploit this is an e−mail message," said Mark Litchfield, director of NGS Software. "If you did it right, you could own every Outlook user in the world within a week," he said.
Source: http://www.techweb.com/wire/security/175803652;jsessionid=KS
BY2QFNY1BIQQSNDBOCKHSCJUMEKJVN

44. *January 11, Beta News* — **Symantec found using rootkit feature.** Symantec is cleaning up a feature in Norton SystemWorks that uses a rootkit−like technique to hide a system folder from Windows. The technology works similar to Sony BMG's controversial rootkit DRM in the way it masks files and makes them invisible to the operating system. The Norton Protected Recycle Bin feature adds a directory called NProtect, which stores temporary copies of files that users delete. The idea was to supplement the standard Windows Recycle Bin and enable users to recover files they removed accidentally. However, hiding a directory from Windows can open

the door to vulnerabilities, as the Sony DRM rootkit debacle exposed. Malware authors were able to write viruses and worms that hid in the cloaked directory, effectively preventing scanning software from discovering their existence on a PC. Users of Norton SystemWorks can download the patch now through LiveUpdate. The rootkit−like activity was discovered by Mark Russinovich of Sysinternals, who first released details on the Sony XCP software.
Source: http://www.betanews.com/article/Symantec_Found_Using_Rootkit_Feature/1137029426

45. *January 09, Tech Web* — **IPv6: World's largest technology upgrade on deck.** Bugs, spam, viruses, software security issues, quality of service and more have spurred experts to push for commercial deployment and government reform on Internet Protocol version 6 (IPv6). A panel battled the topic of when companies should deploy IPv6 and where the technology will make the greatest impact. The discussion took place at the 2006 International Consumer Electronics show in Las Vegas, NV, last week. In the end, the four panelists agreed to disagree. IPv6, the latest version of Internet Protocol, provides more IP addresses than today's version 4. It supports auto−configuration to help correct most shortcomings in the current version, and has security, quality of service, digital rights management and mobile communications features. The debate has heated up in the U.S. now that Asian countries are mandating adoption where IP addresses are in short supply. The U.S. government and the Department of Defense, two of IPv6's strongest proponents, are estimated to spend billions to make the transition happen. The White House Office of Management and Budget has directed U.S. federal agencies to develop IPv6 transition plans by February and requires that agencies comply with the mandate by June 2008.
Source: http://www.compliancepipeline.com/news/175803121;jsessionid=AYA3DIDAR5V2OQSNDBECKHSCJUMEKJVN

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 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. More information about this vulnerability can be found in the following:

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

Technical Cyber Security Alert TA06−005A− Update for Microsoft Windows Metafile Vulnerability: http://www.us−cert.gov/cas/techalerts/TA06−005A.html

Cyber Security Alert SA06−005A − Microsoft Windows Metafile Vulnerability:

http://www.us−cert.gov/cas/alerts/SA06−005A.html

US−CERT strongly encourages users and administrators to apply the appropriate updates as soon as possible. Microsoft has released an update to address this vulnerability in Microsoft Security Bulletin MS06−001:
http://www.microsoft.com/technet/security/Bulletin/MS06−001. mspx

Microsoft Windows, Outlook, and Exchange Vulnerabilities: US−CERT Cyber Security Alert SA06−010A

Microsoft Security Bulletins for January 2006 address vulnerabilities in Microsoft Windows, Outlook, and Exchange:
http://www.microsoft.com/technet/security/bulletin/ms06−jan. mspx

These vulnerabilities may allow an attacker to take control of your computer or cause it to crash. System affected:

Microsoft Windows
Microsoft Outlook
Microsoft Exchange

The following references are provided: US−CERT Technical Cyber Security Alert TA06−010A.html − http://www.us−cert.gov/cas/techalerts/TA06−010A.html

US−CERT Vulnerability Note VU#915930 − http://www.kb.cert.org/vuls/id/915930

US−CERT Vulnerability Note VU#252146 − http://www.kb.cert.org/vuls/id/252146

Microsoft Security Bulletin Summary for January 2006 −
http://www.microsoft.com/technet/security/bulletin/ms06−jan. mspx

Microsoft Update − https://update.microsoft.com/microsoftupdate/

Security Essentials − http://www.microsoft.com/athome/security/protect/default.asp x

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 27015 (halflife), 139 (netbios−ssn), 32801 (−−−), 135 (epmap), 7008 (afs3−update), 16830 (−−−) 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

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