Department of Homeland Security Daily Open Source Infrastructure Report for 29 November 2005

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

Daily Highlights

- The News & Record reports North Carolina has passed a new law to help in identity theft defense which will allow people to put a freeze on their credit reports and prevent government agencies and businesses from using a Social Security number as an employee identification number. (See item 5)
- eWeek reports Verizon Wireless is suing Passport Holidays of Florida for using an automated dialer to send unwanted text messages to 98,000 Verizon Wireless customers in three East Coast area codes. (See item 22)

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. *November 28, Reuters* — **OPEC plans to prevent price spike.** The Organization of the Petroleum Exporting Countries (OPEC) will pump enough oil to build up global stockpiles and cushion consumers in the United States, Europe and Japan from higher prices this winter, the producer group's president said on Monday, November 28. OPEC has been producing nearly flat out at 30 million barrels per day (bpd) for months as it seeks to fill storage tanks and tame prices that went above $70 in August. Swelling inventories have cut $13 off oil since then, but OPEC President Sheikh Ahmad al−Fahd al−Sabah, also Kuwaiti oil minister, said producers

want stockpiles to rise higher still. “We are allowing the stocks to build as OPEC, since last year. We are trying to make stocks build even to 56 days (of forward demand cover),” said Sheikh Ahmad told reporters. “For this is one of the points that we think will be very important to stabilize prices,” he said. OPEC previously described 56 days of forward demand cover as excessive, however, analysts said OPEC's stock−piling plan, however well−intentioned, cannot relieve tightness in refined oil products such as heating oil and gasoline.
Source: http://www.nytimes.com/reuters/business/business−energy−saud i−naimi.html

2. *November 28, NBC 4 (OH)* — **Thousands without electricity after explosion at power station.** American Electric Power officials said it could take up to two days to fully restore electricity after a substation in Columbus, OH, exploded Monday, November 28, leaving at least 32,000 customers on the city's north side without power. The explosion and resulting fire brought down large power lines, causing damage that could take days to repair. Two of three transformers at the substation caught on fire.
Source: http://www.nbc4i.com/news/5415807/detail.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *November 28, WBNS TV (OH)* — **Unknown source of foul order prompts resident evacuation in Ohio.** Authorities still don't know the source of a foul odor that prompted an evacuation in southeast Ohio Saturday night, November 26. Hundreds of people were forced to leave their homes for several hours in Chauncey, a village outside Athens, OH. Firefighters and a Hazmat response team tried to figure out where the smell was coming from but couldn't find a chemical spill, gas leak or other source. However, Athens County sheriff's deputy John Morris says two firefighters were taken to a hospital after they felt lightheaded and dropped to their knees. The Chauncey−Dover fire chief says residue is now being analyzed from a burned spot in a vacant lot where a woman says she saw white smoke rising on Saturday.
Source: http://www.10tv.com/Global/story.asp?S=4168449&nav=LUER

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *November 28, UK Financial Sector Continuity* — **UK financial sector participates in market wide exercise.** The UK financial sector took part in the largest ever market wide test of its preparedness to respond to a major crisis such as a terrorist attack, natural disaster or widespread infrastructure damage on Monday, November 28. The desk−based exercise was organized by the financial stability teams at the Tripartite Authorities (HM Treasury, the Bank of England and the Financial Services Authority) who would have responsibility for overseeing

and coordinating the markets response to such an incident. More than 1,000 people, from the Tripartite Authorities and some 80 organizations across the UK took part. The test, which was designed to be as realistic as possible, involved a scenario of widespread disruption in London and other financial centers, and included simulated news broadcasts, interviews and market and currency movements. KPMG will report early in 2006 on the effectiveness of the sector's business continuity preparations and the Authorities' contribution. A report on the findings together with any recommendations for improvements will be published.
Source: http://www.fsc.gov.uk/section.asp?catid=349&docid=947

5. *November 28, News & Record (NC)* — **North Carolina boosts identity theft defense.** Among the dozens of new laws in North Carolina that will go into effect Thursday, December 1, is one designed to make it easier for North Carolinians to protect themselves against identity theft. "Come December 1, North Carolina will be among the few states in the country that allow people to put a freeze on their credit report," state Attorney General Roy Cooper said. "This can be an important way to prevent identity theft to begin with," said Cooper. Under the new law, residents can send a certified letter to each of the credit−reporting agencies asking that their credit be frozen. Then, even if someone does steal their personal information, the thief won't be able to open a new account. Credit−reporting agencies already do this for people who have been victims of identity theft, but not for people who are trying to prevent fraud. North Carolina's new identity theft law also orders government agencies and businesses to stop taking Social Security numbers when they're not needed and prevents them from using a Social Security number as an employee identification number, Cooper said.
Source: http://www.news−record.com/apps/pbcs.dll/article?AID=/20051128/NEWSREC0101/511280304/−1/NEWSRECRSS

6. *November 28, Reuters* — **Cybercrime yields more cash than drugs according to expert.** Global cybercrime generated a higher turnover than drug trafficking in 2004 and is set to grow even further with the wider use of technology in developing countries, a top expert said on Monday, November 28. No country is immune from cybercrime, which includes corporate espionage, child pornography, stock manipulation, extortion and piracy, said Valerie McNiven, who advises the U.S. Treasury on cybercrime. "Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion," said McNiven. Asked if there was evidence of links between the funding of terrorism and cybercrime, McNiven said: "There is evidence of links between them. But what's more important is our refusal or failure to create secure systems, we can do it but it's an issue of costs." Developing countries which lack the virtual financial systems available elsewhere are easier prey for cybercrime perpetrators, who are often idle youths looking for quick gain. "When you have identity thefts or corruption and manipulation of information there (developing countries), it becomes almost more important because ... their systems start getting compromised from the get−go," she said.
Source: http://today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2005−11−28T200056Z_01_KWA867007_RTRUKOC_0_US−CYBERCRIME.xml&archived=False

7. *November 25, Internetnews.com* — **Correctly identifying fraudulent e−mail can be difficult for users.** Knowing the difference between a legitimate e−mail and a scammed phishing e−mail is not always as easy as one would think. According to data from e−mail security firm

MailFrontier, only four percent of users can spot a phished e−mail 100 percent of the time. MailFrontier's data comes from its Phishing IQ Test, which is comprised of 10 examples of e−mails and users must choose whether they think the mail is legitimate, a fraud or if they have no answer. The average score in 2005, according to MailFrontier, is 75 percent, which is up from 61 percent in 2004. One of the surprising results of the survey, according to Andrew Klein, manager with the MailFrontier Threat Center, is that younger people (18−24) are more likely than older people (55+) to be fooled by a phishing attack.
Source: http://www.internetnews.com/security/article.php/3566071

[Return to top]

Transportation and Border Security Sector

8. *November 28, Associated Press* — **Monorail crash investigation to focus on three scenarios.** Investigators will focus on three possible causes for the monorail crash: operator error, signal malfunction, or communications problems, officials said Sunday, November 27. The 43−year−old elevated line's only two trains remained stuck on the tracks in downtown Seattle on Sunday as 15,000 people ran underneath in the Seattle Marathon and thousands of shoppers and cars passed under the tracks after the race. The trains have been stuck on a curve about 30 feet above Fifth Avenue near Westlake Center since crashing shortly after 7 p.m. PST Saturday, November 26. Perry Cooper, Seattle Center spokesperson said police, fire and transportation officials are working with crane and towing companies to find the best way to return the trains to the Seattle Center station, where the monorail maintenance facility is located. In the past, if one train broke down, the other could be used to tow it. He said the Seattle Center, which has run the monorail since it was built for the 1962 World Fair, has never dealt with two disabled trains at the same time. Investigators from the state Department of Transportation and the National Transportation Safety Board need to figure out what part of the system failed
Source: http://159.54.227.3/apps/pbcs.dll/article?AID=/20051128/NEWS 06/51128040

9. *November 28, Associated Press* — **Barge runs aground, leaks chemical into James River.** Officials say liquid asphalt has been leaking out of a barge that ran aground Monday, November 28, in the James River. According to the U.S. Coast Guard, the barge −− called the Piney Point −− was carrying over a million gallons of liquid asphalt, but only one tank containing about 120 thousand gallons was leaking. Lieutenant Gary Hutchison with the Henrico County, VA, Fire Department says the barge ran aground about five miles south of Richmond, near the Henrico/Chesterfield county line, around 4:30 a.m. EST. Hutchison says county officials called in the Coast Guard, the Virginia Department of Emergency Management, and the Environmental Protection Agency to help.
Source: http://www.wavy.com/Global/story.asp?S=4171018&nav=23ii

10. *November 17, Department of Transportation* — **Grant helps launch Florida 511 service.** Florida drivers can now call 511 for up−to−the minute updates on traffic jams, road construction, lane closures, severe weather and travel times on Interstates and major highways. Florida Department of Transportation Secretary Denver Stutler unveiled the 511 service as part of a new information technology system designed to cut congestion and improve safety on Florida highways. In addition to the 511 service for drivers, the new system helps Florida transportation officials better respond to changes in traffic conditions, accidents and other

highway trouble spots. The 511 system also will serve as an invaluable tool during hurricane season when the most current highway information is especially crucial, according to Acting Federal Highway Administrator J. Richard Capka. The Federal Highway Administration report also helps states adapt traffic−fighting solutions to local road conditions. The report shows that accidents, construction zones, bad weather, special events, and poor signal timing cause about 60 percent of highway delays.
Federal Highway Administration report:
http://www.ops.fhwa.dot.gov/congestion_report/index.htm
Source: http://www.dot.gov/affairs/fhwa1305.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

11. *November 28, Pennsylvania Ag Connection* — **Plum Pox quarantine lifted in York County Township.** Pennsylvania Agriculture Secretary Dennis Wolff announced that a quarantine for the Plum Pox Virus, a disease that severely affects fruit production, has been rescinded in Conewago Township, York County, PA, and the ban on the planting or selling of stone fruit trees has been lifted. Infected fruit may appear deformed or blemished and could drop prematurely from trees, but causes no harm to animals or people who eat the fruit. The virus was discovered in Conewago Township during the summer of 2002. Wolff said, "We have a strong surveillance and eradication program for Plum Pox and we are aggressively working to eliminate the disease...We've tested more than 925,000 samples in the four−county quarantine area since 2000 as part of the Plum Pox Surveillance Program...We've seen a decline in Plum Pox since then." The department recently completed its sampling and testing for 2005 and found only five positive Plum Pox samples of the more than 269,000 samples taken. The five virus−positive trees, all in Menallen Township, Adams County, were destroyed, along with about 120 acres of stone fruit trees. The quarantine boundaries will change to include an additional portion of Menallen Township, an area adjacent to Bendersville.
Source: http://www.pennsylvaniaagconnection.com/story−state.cfm?Id=6 26&yr=2005

12. *November 27, Bozeman Daily Chronicle (MT)* — **Feedgrounds cause conditions ripe for brucellosis and chronic wasting disease epidemic.** Although the state of Wyoming feeds thousands of elk every winter −− mostly on federal land −− the U.S. Forest Service has never undertaken a formal study of the program, even though most scientists agree the program fosters brucellosis. "When hundreds of elk are crowded together as they are on Wyoming's elk feedgrounds, conditions are ripe for a wildlife disease epidemic," said Lloyd Dorsey, of the Greater Yellowstone Coalition. Brucellosis exposure rates run as high as 50 percent on some feedgrounds, compared to one percent to four percent in herds that find their own food. Chronic wasting disease −− detected in two deer in October near Thermopolis −− is also a problem. "Feedgrounds provide nearly ideal conditions for (chronic wasting disease) transmission among

free−roaming elk," wrote Markus Peterson, a wildlife disease scientist at Texas A&M University, in a report released this month. If feedgrounds were phased out, causing elk to start wandering, brucellosis−infected elk could infect cattle herds and destroy haystacks and crops. One Wyoming cattle herd has already been infected by an elk. Wyoming has announced it will begin an experimental "test and slaughter" program to capture and test elk for the disease.
Source: http://www.bozemandailychronicle.com/articles/2005/11/27/new s/01elk.txt

[Return to top]

Food Sector

13. *November 28, Food Production Daily* — **European Union scientists call for listeria alert network for food.** Improved surveillance can identify and halt potentially large outbreaks of listeria. According to a study conducted by the European Union (EU), outbreaks of listeriosis lead to the death of about 20 percent to 30 percent of those infected. "Changes in the way food is produced, distributed and stored have created the potential for diffuse and widespread outbreaks involving many countries," the authors stated. Public health authorities do not always recognize the prominence of listeriosis in causing infection, particularly since it is a relatively rare disease compared with other common foodborne illnesses such as salmonellosis. Listerosis ranks as the second leading cause of fatalities from foodborne diseases after salmonellosis in the U.S. and France. Several countries still have high incidence, and many do not have a surveillance system. "Moreover, its common source epidemic potential presents a real threat and persists even in countries with a decreasing or low incidence," they stated. Between 1991 and 2002, 19 outbreaks of invasive listeriosis were reported in nine different countries, with a total of 526 outbreak related cases. The incriminated products for six of these outbreaks were known to have been exported.
Study: http://www.eurosurveillance.org/em/v10n10/1010−225.asp
Source: http://www.foodproductiondaily.com/news/ng.asp?n=64185−liste ria−poultry−food−safety

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

14. *November 28, Xinhuanet (China)* — **Virus mutation found in human bird flu cases.** Studies show the H5N1 strain of virus separated from China's human cases of bird flu has mutated compared with the strain found in Vietnam's human cases, said the Chinese Ministry of Health (MOH) on Monday, November 28. Lab tests find the H5N1 strain of virus separated from recent human cases is highly homologous with that found in poultry samples from the bird flu outbreak places, according to the information office of the MOH. However, compared with the virus strain from the human cases in Vietnam, the genetic order of H5N1 in China's human

cases has mutated "to a certain degree," the MOH spokesperson Mao Qun'an said. "But the mutation is impossible to cause human−to−human transmission of the avian flu," he noted. China has reported three confirmed human cases of bird flu, including two fatalities from east China's Anhui Province and one case from the central Hunan Province in which the patient has recovered.
Source: http://news.xinhuanet.com/english/2005−11/28/content_3848013 .htm

15. *November 28, Australian Associated Press* — **Australia to co−host bioterror workshop.** Australia and Indonesia will co−host a second regional workshop on the Biological Weapons Convention in a bid to further reduce the threat of bioterrorism. Australian Defense Minister Robert Hill said the workshop, to be held in Indonesia early next year, followed a preliminary workshop held in Melbourne, Australia, in February. Hill said it was part of ongoing efforts to reduce the possibility of terrorists acquiring and using biological weapons. It also aims to prevent regional nations from inadvertently helping the development of biological weapons programs elsewhere. Regional neighbors will be invited to the meeting. The Biological Weapons Convention prohibits member states developing, producing, stockpiling or otherwise acquiring or retaining biological weapons or their means of delivery.
Source: http://seven.com.au/news/nationalnews/124759

16. *November 27, Press Association* — **Australia to stage bird flu test.** Australia will stage its first major test of its preparedness for a bird flu outbreak. The four−day Exercise Eleusis starting on Tuesday, November 29, will involve 1,000 people from the federal and state governments, agriculture and health departments as well as the agriculture industry, Agriculture Minister Peter McGauran and Health Minister Tony Abbott said in a joint statement. Australia has yet to detect a case of the lethal H5N1 strain of the bird flu virus that has killed at least 68 people and ravaged poultry populations in Asia. The federal government is coordinating preparations for an outbreak among Australian birds as well for a potential pandemic if the virus mutates into a form that spreads easily among humans. McGauran said the drill would use a hypothetical scenario to test how well agriculture and health departments work with industry to identify, contain and eradicate an outbreak among birds. Abbott said the exercise scenario included human victims of the disease.
Source: http://news.scotsman.com/latest.cfm?id=2311842005

17. *October 25, PLoS Biology* — **Wave−like spread of Ebola.** In the past decade the Zaire strain of Ebola virus (ZEBOV) has emerged repeatedly into human populations in central Africa and caused massive die−offs of gorillas and chimpanzees. Researchers tested the view that emergence events are independent and caused by ZEBOV variants that have been long resident at each locality. Phylogenetic analyses place the earliest known outbreak at Yambuku, Democratic Republic of Congo, very near to the root of the ZEBOV tree, suggesting that viruses causing all other known outbreaks evolved from a Yambuku−like virus after 1976. The tendency for earlier outbreaks to be directly ancestral to later outbreaks suggests that outbreaks are epidemiologically linked and may have occurred at the front of an advancing wave. Distances among outbreaks indicate a spread rate of about 31 miles per year that remains consistent across spatial scales. Viral evolution is clocklike, and sequences show a high level of small−scale spatial structure. Genetic similarity decays with distance at roughly the same rate at all spatial scales. Analyses suggest that ZEBOV has recently spread across the region rather than being long persistent at each outbreak locality. Controlling the impact of Ebola on wild

apes and human populations may be more feasible than previously recognized.
Source: http://biology.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.pbio.0030371

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

18. *November 28, Japan Times* — **Nuclear attack response tested in Japan.** The Japanese government Sunday, November 27, conducted its first exercise under a new law designed to protect the public in the event of an attack, based on a scenario involving a terrorist strike on a nuclear power plant in Mihama, Fukui Prefecture in Japan. About 1,300 people from 130 organizations, including municipalities, police, the Self−Defense Forces, electric power firms and local broadcasters, participated in the exercise. The scenario involved mortar attacks on the Mihama nuclear power plant by unidentified terrorists, damaging the plant's No. 2 reactor and raising fears of a radiation leak. Fukui was selected as the venue for the first exercise because the prefecture, which has 15 nuclear power plants, drew up contingency plans immediately after the law was enacted in September 2004. The aim of the drill was to see whether the law is effective in getting residents evacuated safely. The law stipulates the authority and roles of national and local governments in protecting the lives and assets of citizens in the event of an emergency. It restricts some civil liberties, such as allowing authorities to commandeer private land and buildings in connection with the evacuations, and gives authorities some control over media organizations.
Source: http://www.japantimes.co.jp/cgi−bin/getarticle.pl5?nn2005112 8a3.htm

19. *November 27, Washington Post* — **Streamlined emergency operations center being built in Virginia county.** The road to a new, state−of−the−art communications center began on Monday morning, November 21, in Fairfax County, VA, with a groundbreaking ceremony at the site. In addition to Fairfax police and fire departments, the center will house the county's emergency operations center as well as dispatchers for the Virginia State Police and the Virginia Department of Transportation. Law enforcement and government officials said the 130−acre site should become a model for other areas looking to combine their key communications in one spot. Fairfax's center also will eventually house bus maintenance facilities for Metro and the Fairfax Connector, as well as the regional barracks for the state police. County Executive Anthony H. Griffin said the communications and emergency center is scheduled to open in November 2007, but an additional four to six months will be needed to finish wiring and testing the technology in the building.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/11/25/AR2005112501511.html

[Return to top]

Information Technology and Telecommunications Sector

20. *November 28, InfoWorld* — **Sober variant on rise, security firm warns.** The latest variant of the Sober worm is proliferating, with a staggering one in 14 e−mails circulated on the Internet containing it as of Monday morning, November 28, according to the antivirus vendor Sophos. Around 85 percent of all viruses reported to Sophos are what the company calls Sober−Z, up from around 60 percent last week, said Graham Cluley, senior technology consultant. Right now, Sober−Z ranks as the third most prevalent virus for the year, behind Netsky−P in first and Zafi−D in second, he said. It first appeared around November 22 using several forms of social engineering to trick users into executing the attachment. Messages purporting to be from the U.S. Federal Bureau of Investigation warn recipients that they have been visiting illegal Websites and ask them to read a list of attached questions. Other versions pretend to be from the U.S. Central Intelligence Agency or offer video clips of Paris Hilton and Nicole Richie from the TV show "The Simple Life." While most antivirus vendors have updates that can remove the worm, the "clever" social engineering ploys are still effective, Cluley said.
Source: http://www.infoworld.com/article/05/11/28/HNsobervariantrise_1.html

21. *November 28, Associated Press* — **New protocol said to help blend telecom services.** As easy as it is to connect these days by Internet, cellular, Wi−Fi, and plain old telephones, the networks that make all that possible can't communicate well with one another. Technological standards vary from network to network. The traditional phone system and the Internet use completely different protocols. A new standard, Internet Protocol for Multimedia Services (IMS), is being seen as perhaps the most likely means for linking traditional and wireless communications. But like with all new technology, IMS has issues and is only a springboard for convergence between future services, not today's −− nearly all of which would need to be adapted or replaced over time to enable them to intermingle. Most existing telecom services were designed to perform their specific functions as if walled off into distinct silos on the network. IMS attempts to knock down these silos by introducing a common interface for creating sessions. That way, data can be intertwined or bridged across networks to different devices.
Source: http://www.informationweek.com/story/showArticle.jhtml;jsessionid=2OUFALYBADGEIQSNDBGCKHSCJUMEKJVN?articleID=174401977

22. *November 23, eWeek* — **Verizon Wireless sues another spammer.** Unwanted text messages from a Florida−based travel company were sent recently to 98,000 Verizon Wireless customers, according to a new lawsuit filed by the operator. Even though cell phone spam is still relatively limited, it's nonetheless forcing operators to get a handle on it since their subscribers often pay a fee for each incoming message. "Electronic attacks upon the Verizon Wireless interstate text messaging network will continue; indeed the latest attack was just weeks ago," Verizon attorneys wrote in the suit filed Monday, November 21, in a U.S. District Court in New Jersey. In this particular case, Verizon Wireless alleges that Passport Holidays LLC, of Ormond Beach, FL, sent unsolicited text messages to about 98,000 Verizon Wireless subscribers in the latter part of October. The lawsuit accuses Passport Holidays of using an automated dialer to send the text messages to phones in three East Coast area codes.
Source: http://www.eweek.com/article2/0,1895,1892707,00.asp

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 a publicly reported vulnerability in the way Cisco PIX firewalls process legitimate TCP connection attempts. A remote attacker may be able to send spoofed, malformed TCP packets with incorrect checksum values through affected PIX firewalls. Legitimate network traffic to the destination, PIX protected hosts may be blocked until the invalid PIX connection attempt entry times out around two minutes by default. Until a patch or more information becomes available, US−CERT recommends that system administrators who may be affected consider reconfiguring certain connection timers on Cisco PIX systems. Public exploit code for this reported vulnerability may be useful for automating a sustained attack.

For more information please review the following US−CERT Vulnerability Note (VU#853540):
Cisco PIX TCP checksum verification failure report
http://www.kb.cert.org/vuls/id/853540

Microsoft Distribution Transaction Coordinator (MSDTC) Exploit (MS05−051) The researcher Darkeagle of the unl0ck security group has released a proof of concept denial of service exploit targeting the Microsoft Windows MSDTC Memory Corruption Vulnerability (BID 15056), which was originally discovered by eEye Digital Security and disclosed on October 11, 2005. Although the vulnerability is said to allow for remote code execution, the exploit released will only cause a denial of service. The public release of this tool however may increase the likelihood of a more sophisticated exploit being released.

The exploit can be referenced from the following location
Microsoft Windows Distributed Transaction Coordinator Remote Exploit (MS05−051) http://www.frsirt.com/exploits/20051127.55k7−msdtc.c.php

Administrators are advised to ensure that all relevant updates to Microsoft Windows have been applied, and also that TCP port 3372, which is the default port for MSDTC, be filtered at the network boundary. On October 11, 2005 the DeepSight Threat Analyst Team issued a Threat Alert in response to this vulnerability. Administrators are advised to review its contents and apply all suggested mitigating strategies possible, in the event the patch cannot be applied.

Microsoft MSDTC and COM+ Remote Vulnerabilities Alert
https://tms.symantec.com/members/viewdocument.asp?guid=FCF7359D897F40E7B92082B708AD2B56

W32/Sober Revisited
US−CERT is aware of several new variants of the W32/Sober virus that propagate via email. As with many viruses, these variants rely on social engineering to propagate. Specifically, the user must click on a link or open an attached file. A recent variant sends messages that appear to be from the CIA or FBI, while a German version appears to be coming from the Bundeskriminalamt (BKA), the German Federal police service. Additionally, US−CERT strongly encourages users not to follow unknown links, even if sent by a known and trusted source.

US−CERT encourages users to review the FBI ALERTS PUBLIC TO RECENT E−MAIL SCHEME at URL:
http://www.fbi.gov/pressrel/pressrel05/emailscheme112205.htm

BKA warnt vor gefälschten E−Mails mit BKA−Absender − Variante des Sober−Wurms: http://www.bka.de

US−CERT strongly encourages users to install anti−virus software, and keep its virus signature files up to date.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 80 (www), 27015 (halflife), 139 (netbios−ssn), 135 (epmap), 53 (domain), 25 (smtp), 40000 (−−−) 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

23. *November 28, Associated Press* — **Piece of Supreme Court marble falls near tourists.** A basketball−sized piece of marble fell from the facade over the entrance to the Supreme Court, landing on the steps near visitors waiting to enter the building on Monday, November 28. No one was injured when the stone fell. The marble was part of the dentil that serves as a frame for the frieze of statues atop the court's main entrance. A group of visitors had just entered the building and had passed under the frieze when the stone fell at 9:30 a.m. EST. The 70−year−old Supreme Court building is undergoing a $122 million, five−year renovation project, although it does not appear that the accident was related to that work.
Source: http://www.usatoday.com/news/washington/2005−11−28−supreme−court−marble_x.htm

24. *November 28, Associated Press* — **First New Orleans school opens since Katrina.** Greeted by welcome signs hung over the door and in the hallways, students began returning Monday, November 28, to the first regular public school to reopen since Hurricane Katrina hit three months ago. Enrollment was expected to be about 200 at Ben Franklin Elementary, in the

affluent uptown area that was relatively unscathed by the storm. Before Katrina, it was a math−science magnet school with 390 students from preschool through eighth grade. "This signals that school is up and running, and that's a good thing," Orleans Parish School Board member Heidi Daniels said. Some private schools in New Orleans began reopening in October, but no public schools had opened, with the exception of a few charters that were outside the local board's control.
Source: http://www.usatoday.com/news/nation/2005−11−28−new−orleans−s chools_x.htm

25. *November 23, New York Times* — **Dam at a Catskill Reservoir needs emergency repair.** A massive 78−year−old dam in the Catskill Mountains that is owned by New York City does not meet state safety standards and will have to undergo emergency repairs before next spring's snow melt. Officials said there was a remote possibility that the Gilboa Dam would fail if there was a record storm and snow melt, sending the 20 billion gallons of water in the Schoharie Reservoir roaring through the valley below, a historic area of covered bridges and small farms that is home to about 5,000 people. The New York City Department of Environmental Protection, which owns the 1,800−foot−long dam, has held several meetings with frightened local residents, trying to explain the risk without provoking panic. Emily Lloyd, commissioner of the department said she felt it was necessary to inform residents of the danger and to help them prepare an evacuation plan, though the chance that the dam will fail is remote. Officials said the emergency was based on a question of safety that is caused by a shift in weather patterns, not a sudden deterioration of the dam. There have been scientific indications that the climate of the Northeast is changing and that storms that were once rare are now far more common.
Source: http://www.nytimes.com/2005/11/28/nyregion/28dam.html

[Return to top]

General Sector

26. *November 28, Associated Press* — **Post−holiday travelers stranded in Midwest.** Travelers trying to get home after Thanksgiving were stranded across the Plains on Monday, November 28, as the region's first big snowstorm of the season closed hundreds of miles of highways, cutting visibility to zero and piling up drifts six feet high. Snow driven by wind up to 69 mph fell from North Dakota to the Texas Panhandle, shutting down schools and the South Dakota state government. Four deaths were blamed on slippery roads in South Dakota, Nebraska, and Kansas, and a fifth person was killed when tornado picked up and hurled a car in Arkansas. Numerous other highways also were closed across the Plains, including a 175−mile stretch of I−90 across South Dakota, and a 60−mile stretch of I−80 in Nebraska. Hundreds of travelers were stranded. Wind, snow and ice in South Dakota snapped electrical lines −− coating some cables with ice a few inches thick −− and knocked out power to thousands of customers. In addition, grass fires driven by the storm system's wind blackened thousands of acres in Texas and Oklahoma. Several homes were destroyed in the two states and hundreds of families had to evacuate in Oklahoma.
Source: http://news.yahoo.com/s/ap/20051128/ap_on_re_us/stormy_weather;_ylt=AkCujLtX0109J2RN5oyVMESs0NUE;_ylu=X3oDMTA3MjBwMWtkBHNlYwM3MTg−

[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