Department of Homeland Security Daily Open Source Infrastructure Report for 28 October 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Department of Homeland Security, in collaboration with the Department of Defense and Department of State, announced the completion and final approval for eight plans supporting the National Strategy for Maritime Security. (See item 6)

- The New York Times reports that drug company Roche has temporarily halted shipments of the anti−influenza drug Tamiflu in the U.S., saying it wants to prevent hoarding and ensure adequate supplies to treat conventional flu cases this winter. (See item 10)

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. *October 27, Reuters* — **Coal challenging gas as power plant fuel.** Coal, abundant and easily shipped, is starting to challenge natural gas as the fuel of choice for new power plants. This is because coal prices are relatively cheaper and not so volatile, industry executives and experts say. Utilities around the world have increasingly turned to gas to meet a doubling of electricity demand over the next 25 years, but this is changing. Demand for coal is growing faster than expected, rising 25 percent in the last three years, to 1.1 billion tons. The International Energy Agency (IEA), the West's energy watchdog, says coal will continue to dominate electricity generation with a 40 percent share, as most of the world's supplies are conveniently located in the strongest and fastest growing economies, the United States, China and India. "This is likely

to continue as demand for power grows mainly in the developing economies. But coal must remain competitively priced, especially as pollution abatement costs increase as carbon emission plans increase," said IEA chief Claude Mandil.
Source: http://abcnews.go.com/US/wireStory?id=1255646

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

2. *October 26, Federal Computer Week* — **Defense analysts forecast few new procurements.** The September 11, 2001, terrorist attacks changed everything in the Department of Defense (DoD) and the defense industry, according to an industry executive who spoke about DoD budget trends. With DoD spending now at levels near what they were in the mid−1980s, people can expect to see it slow and then sharply decline by fiscal year 2011, said Cecil Black, a Boeing executive, speaking at the 2005 Vision Conference in Falls Church, VA. The conference, sponsored by the Government Electronics and Information Technology Association, highlighted spending details in DoD's $30.1 billion IT and national security systems budget for fiscal year 2006. Defense analysts said that budget would grow to $34.8 billion in fiscal year 2011. However, they cautioned IT and security industry officials that few "new starts" are planned in an environment shaped now by streamlining and consolidation efforts. In a defense industry recently grown accustomed to burgeoning IT appropriations and supplemental funding, Black said the industries that do well in the future will be those that can offer innovative approaches to slowing or stopping the burden of DoD's operations and maintenance budget. That budget is growing three percent a year faster than inflation.
2005 Vision Conference: http://www.geia.org/index.asp?bid=1015
Source: http://www.fcw.com/article91213−10−26−05−Web

[Return to top]

Banking and Finance Sector

3. *October 27, Associated Press* — **Wisconsin man jailed in hurricane scam.** A man from Green Bay, WI, accused of perpetrating a Hurricane Katrina scam, is jailed on $50 million dollars bond in New Orleans. Scott Benson is charged with extracting personal information from 2,500 police officers and other emergency workers in New Orleans following the hurricane. Benson is booked on 2,500 counts of false impersonation and 2,500 counts of identity theft. Prosecutors say Benson and another man, Christ Armstrong of Orlando, FL, had officers sign application forms that included personal information in order to receive $5,000 dollars from Viacom. The men are accused of planning to use information from the emergency workers to steal disaster assistance that was supposed to go to hurricane victims.
Source: http://www.wbay.com/global/story.asp?s=4036806&ClientType=

4. *October 26, CNET News.com* — **Banks to blacklist rogue workers in fraud fight.** Major U.S. financial institutions are working to set up a new defense against insider fraud: a database of employees who are known to be scam risks. Banks and similar organizations already run reference and background checks on new employees, but an extra security measure is needed, according to BITS, a consortium of 100 of the largest U.S. financial institutions. The new database, announced Wednesday, October 26, will list information on employees at financial institutions who were fired because they compromised customer data or knowingly caused financial losses, the group said. "There is a phenomenon of people being able to literally walk down the street to another financial institution and get hired," said Cheryl Charles, a senior director at BITS. In one case, the same scammer was hired by three institutions, she said. "This new database is going to help prevent that kind of thing," said Charles. Reports of insiders attacking financial services systems are on the increase. In a 2004 Deloitte survey of IT security in the industry, 35 percent of companies said they had come under an attack from an internal source. That's up from 14 percent in 2003.
Source: http://news.com.com/Banks+to+blacklist+rogue+workers+in+fraud+fight/2100−1029_3−5915678.html?tag=nefd.top

5. *October 20, The Montclair Times (NJ)* — **University error raises risk of identity theft.** A mistake made by a Montclair State University (MSU) employee has put more than 75 percent of the university's undergraduates at risk for identity theft. For the past five months, the Social Security numbers of 9,100 MSU undergraduates were searchable by Internet search engines. The university was advised of the problem on October 7 when a student, who found his personal information online after an Internet search, contacted MSU's Information Technology Department. According to Ann Frechette, MSU's executive director of communications and marketing, a university employee accidentally stored the Social Security numbers and declared majors of the students on MSU's Web server. The employee, Frechette said, believed the files were secure, or nonsearchable, because they were not linked onto the university's Website. "But in fact, anything stored on the Web server is searchable by Web engines," Frechette said. Working with the New Jersey State Attorney General's Office, the university was able to remove all files from Internet caches by October 12, five days after the university was notified about the problem. MSU is located in Montclair, NJ.
Source: http://www.montclairtimes.com/page.php?page=10627

[Return to top]

Transportation and Border Security Sector

6. *October 26, Department of Homeland Security* — **National Strategy for Maritime Security supporting plans announced.** The Department of Homeland Security, in collaboration with the Department of Defense and Department of State, announced the completion and final approval for eight plans supporting the National Strategy for Maritime Security. These plans include: Maritime Commerce Security, Maritime Transportation Systems Security, Maritime Infrastructure Recovery, Maritime Operational Threat Response, Maritime Domain Awareness, Global Maritime Intelligence Integration, and Domestic and International Outreach. In December 2004, President Bush signed a maritime policy security directive outlining his vision for a fully−coordinated U.S. government effort to protect U.S. interests in the maritime domain.

This security directive resulted in the first−ever, comprehensive National Strategy for Maritime Security. The eight supporting plans work together to enhance international cooperation while maximizing domain awareness that will create necessary layers of security intended to stop terrorists and other threats against the U.S. A team representing more than 20 government agencies contributed to the development of the National Strategy for Maritime Security and its supporting plans. Working groups for the Maritime Commerce Security, Maritime Transportation Systems Security and Maritime Infrastructure Recovery plans also sought public and private sector insight to ensure that those plans reflected maritime industry concerns and knowledge.
National Strategy for Maritime Security:
http://www.dhs.gov/interweb/assetlibrary/HSPD13_MaritimeSecu rityStrategy.pdf
Key elements of the Maritime Security Policy:
http://www.dhs.gov/dhspublic/interapp/editorial/editorial_05 97.xml
Source: http://www.dhs.gov/dhspublic/display?content=4908

7. *October 26, Dallas Morning News (TX)* — **U.S., Canada taking a harder line at border.** The stream of U.S.−bound 18−wheelers and passenger vehicles approaching the customs booths at the Peace Bridge roll through unobtrusive radiation detectors that arch over the inspection lanes. The detectors, designed to sniff out nuclear and radiological hazards, offer silent witness to how the business of commerce and security has changed immensely along what's known as the world's largest undefended border. At the Peace Bridge, the border's third−busiest commercial crossing, U.S. inspectors use a gamma−ray scanner to scrutinize vehicles they suspect could hold contraband cargo or illegal crossers. Rail traffic also passes through a gamma−ray scanner. Motion sensors and digital closed−circuit TV cameras have been deployed at the international bridges, and remote−controlled day− and night−vision cameras keep watch along the Niagara River. Truckers and travelers who have gone through background checks roll through dedicated crossing lanes, their information beamed to the inspections booth in advance. Law enforcement agencies in both countries have stepped up helicopter and boat patrols. "In light of 9−11, there's been a lot more security enforcement on both sides," Darrin Forbes, acting sergeant in charge of the Niagara Regional Police marine unit, said during a recent river patrol. the Peace Bridge, located between Fort Erie, Ontario, and Buffalo, NY.
Source: http://www.dallasnews.com/sharedcontent/dws/news/world/stori es/DN−canada_26int.ART0.State.Edition2.7260b3d.html

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

8. *October 27, Sioux City Journal (IA)* — **College to host animal disease training.** Western Iowa Tech Community College will host a free one−day program November 3 that provides infectious animal disease response training. Sponsored by the Iowa Department of Agriculture

and Land Stewardship, the Iowa Department of Natural Resources, and the Iowa Homeland Security and Emergency Management Division, the program will run from 8 a.m. to 3:30 p.m. in the Large Lecture Hall at the Sioux City campus. The training is designed for local emergency management agencies, fire officials, law enforcement officials, community leaders, public health officials, emergency medical services professionals, representatives of the agriculture industry, farmers and other agricultural producers, veterinarians and agriculture educators.
Source: http://www.siouxcityjournal.com/articles/2005/10/27/news_business/local/5cacfedc796c9d65862570a7000b7803.txt

[Return to top]

Food Sector

9. *October 27, USAgNet* — **Labeling proposal delayed.** Grocery shoppers will have to wait two more years for labels telling where their meat comes from, under a bill moving toward approval in Congress. Originally proposed for 2004, mandatory meat labeling is opposed by meatpackers and supermarkets who say it's a record−keeping nightmare. House−Senate negotiators agreed Wednesday, October 26, to postpone it until 2008. Labeling went into effect last April for fish and shellfish. The delay is part of a $100 billion spending bill for food and farm programs for the budget year that began October 1. The House and Senate passed different versions of the bill, and a conference committee signed off Wednesday, October 26, on a final version. Country of origin labeling (COOL) implementation is now delayed until September 30, 2008.
Source: http://www.usagnet.com/story−national.cfm?Id=1076&yr=2005

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

10. *October 27, New York Times* — **Hoarding prompts halt in flu drug shipping.** Roche has temporarily halted shipments of the anti−influenza drug Tamiflu in the U.S., saying it wants to prevent hoarding and ensure adequate supplies to treat conventional flu cases this winter. Roche said companies had been creating their own stockpiles for use by their employees in the event of a pandemic caused by avian flu. That activity threatened to deplete supplies needed for the regular flu. "At the present time, we do not have an avian influenza pandemic in the U.S.," George Abercrombie, president of the company's American subsidiary, said in a statement Wednesday, October 26. "However, we need to make sure that people exposed to this year's seasonal flu virus will have access to Tamiflu." Roche, which is based in Switzerland, said it would resume shipments of the drug when more flu cases occurred this winter. The halt in shipments affects those to wholesalers and pharmacies but not those to the federal government for its stockpile. The drug, also known as oseltamivir, can reduce the duration of conventional

flu or prevent it. Scientists say it should also work, though perhaps not as well, against the avian flu that has killed more than 60 people in Asia.
Source: http://www.nytimes.com/2005/10/27/health/27flu.html

11. *October 27, Agence France Presse* — **Indonesia, puzzled over bird flu cases, investigates cats as spreaders.** Indonesia's human bird flu outbreak is puzzling experts because several victims do not work or live around poultry, prompting an investigation into whether other animal hosts, perhaps cats, are to blame for the disease's spread. The World Health Organization (WHO) says the lethal H5N1 strain of bird flu that has killed more than 60 people in Asia since late 2003 is mostly transmitted to humans through direct contact with infected birds or their droppings. But Indonesian Health Minister Siti Fadilah Supari has said there is so far no evidence of most of the country's victims catching the virus through close contact with, or eating the meat of, infected birds. "We can only suspect that those infected, contracted the virus through the droppings or contact with the saliva of infected birds or fowl," said Suyono, from the health ministry's bird flu department. Suyono says it is a mystery how several people confirmed to have bird flu in Indonesia contracted H5N1 when they lived in and around urban Jakarta. "Worldwide, more than 80 percent of infections can be traced back to contact with poultry," said Indonesia's WHO representative Georg Petersen, saying the body was not yet concerned that animals such as cats may be spreading the disease.
Source: http://news.yahoo.com/s/afp/20051027/hl_afp/healthfluindonesia_051027113947;_ylt=Avd768Sx09rrar6HQZg57PqJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

12. *October 26, Agence France Presse* — **Russian scientists working on vaccine against smallpox.** Russian scientists are working on an oral vaccine against smallpox, fearing that terrorists could use the virus as a weapon, the head of the Russian Association of Biotechnologies Experts said. Vaccination against smallpox, which the World Heath Organization (WHO) discontinued in 1980, must be resumed "because of the growing threat posed by bioterrorism," Anatoly Vorobyov was quoted as saying by ITAR−TASS news agency. Russian scientists have resumed research on the prototype of a smallpox vaccine pill which was elaborated 30 years ago, said Vorobyov, a member of Russia's Medical Sciences Academy. "Chemical tests will begin soon. (The vaccine's) efficiency on animals has been established, it still needs to be tested on humans," Vorobyov said. WHO announced in 1979 that smallpox had been eradicated from the face of the Earth thanks to a worldwide vaccination campaign. Vaccination was discontinued May 8, 1980.
Source: http://news.yahoo.com/s/afp/20051026/hl_afp/russiahealthterrorism_051026215217;_ylt=Auu2JDKhkZD7f9jhUHQHQH6JOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

13. *October 26, Government Health IT* — **Improved global disease surveillance systems needed.** Health ministers and delegates from more than 30 countries and international health organizations meeting in Ottawa, Canada, have called for increased efforts, including improved disease surveillance systems, to prepare for a possible flu pandemic. The delegates said monitoring the H5N1 strain of influenza, known as bird flu, is essential. They agreed that the immediate global public health issue "is to work collaboratively with the animal health sector to prevent and contain the spread of the H5N1 virus among animals and from animals to humans." The ministers said efforts to prevent a pandemic will require "collaboration and support

between countries in developing national and regional plans for avian influenza control and pandemic influenza preparedness within the framework of a coherent international risk management approach." Disease surveillance and early detection, diagnosis reporting and rapid response, are crucial to preventing the spread of infectious diseases, the delegates said. They urged the development of enhanced, harmonized surveillance systems worldwide. The ministers also called for national pandemic preparedness plans and information−sharing protocols among countries and multilateral organizations.
Source: http://govhealthit.com/article91209−10−26−05−Web

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

14. *October 27, Associated Press* — **Schools evacuated in mock nuclear drill.** The schools close to the Vermont Yankee nuclear power plant near Brattleboro, VT, were evacuated Thursday morning, October 27, in a surprise drill. Officials say 66 buses and two vans were dispatched to 20 schools. About 3,770 students were evacuated from the public and private schools. During the first drill last year, one thousand Vermont students couldn't be evacuated from schools because of a shortage of school buses.
Source: http://www.wrgb.com/news/regional/regional.asp?selection=art icle_42137

15. *October 27, Ukiah Daily Journal (CA)* — **Mendocino County awarded federal grant for school readiness.** The Mendocino County, CA, Office of Education has been awarded a $931,644 grant by the United States Office of Education to help public and private schools in the region better prepare for emergencies and disasters. The grant was developed with input from local stakeholders including police, fire, public health and educators. The 18−month project −− which began October 1 and goes through March 2007 −− is intended to prepare schools to be compliant with state and federal laws that require school staff and teachers to be trained and to serve as emergency service workers who will be activated and on−call in case of a declared local, state and/or national emergency. Classroom safety is only one aspect of being prepared, the superintendent said. Knowing how to secure facilities after an emergency or disaster is another. The project's ultimate impact is intended to improve the safety and security of students through an integrated system of schools, local community, first responders, public agencies, business partners and County Offices of Emergency Services. Officials stressed that not only will this make for safer schools, but safer communities, and will also make life easier on emergency personnel.
Source: http://www.ukiahdailyjournal.com/Stories/0,1413,91~3089~3107 839,00.html

16. *October 27, Advocate Messenger (KY)* — **FEMA drill tests Kentucky county's preparedness.** A simulated chemical emergency at Blue Grass Army Depot in Richmond kept emergency personnel busy in Lancaster on Wednesday morning, October 26. At 9:50 a.m. CDT

the BGANS phone rang. "It stands for Blue Grass Alert Network System," said David East. East, public information officer for Garrard County Emergency Management, was joined in the City Hall meeting room by 11 other emergency personnel involved in the annual Chemical Stockpile Emergency Preparedness Program (CSEPP) drill. Two Federal Emergency Management Agency (FEMA) evaluators roamed with clipboards watching the exercise in action. A semi−circular table was set up with laptop computers logged into a system linking them to emergency alert messages, as well as a chat room and updates keeping them in close contact with all included in the drill. Participants included Madison, Estill, Clark, Powell, Jackson, Rockcastle, Laurel, Jessamine and Fayette counties' Emergency Management personnel, first responders and volunteers, Blue Grass Chemical Activity and Blue Grass Army Depot personnel, and state Emergency Management officials. At the end of the drill, East said, "Everything went fine, and they didn't have any recommendations. We did good."
Source: http://www.amnews.com/public_html/?module=displaystory&story_id=17242&format=html

[Return to top]

Information Technology and Telecommunications Sector

17. *October 27, Secunia* — **SGI issues multiple updates for advanced Linux environment.** SGI has issued updates to fix vulnerabilities in Linux. The vulnerabilities can be exploited to gain escalated privileges, gain knowledge of sensitive information, bypass certain security restrictions, and compromise a user's system. Secunia reports that SGI has issued a patch for SGI Advanced Linux Environment.
Patch 10235 for SGI ProPack 3 Service Pack 6: http://support.sgi.com/
Source: http://secunia.com/advisories/17335/

18. *October 27, Vnunet.com* — **PC awareness program launched in the United Kingdom.** The UK's National Hi−Tech Crime Unit has teamed with the IT industry to launch an awareness program to increase understanding about PC security. The program, "Get Safe Online," is a joint initiative among the government, the National Hi−Tech Crime Unit, and private sector sponsors including BT, Dell, eBay, HSBC, Lloyds TSB, Microsoft, MessageLabs, securetrading.com, and Yell.com. A report released to coincide with the program's launch found that over three quarters of the UK's population (83 percent) don't know enough about protecting themselves online, and that 42 percent of the population just rely on friends and family for online safety advice rather than finding expert information for themselves.
Get Safe Online: http://www.getsafeonline.org./
Source: http://www.vnunet.com/vnunet/news/2144889/national−campaign− targets−pc

19. *October 26, News.com* — **Zotob damage deep but not widespread.** Fewer businesses fell victim to the Zotob worm that struck corporate networks in August than previous attacks, according to a report released on Wednesday, October 26, by computer security firm Cybertrust. Of 700 organizations surveyed, 13 percent were disrupted by the worm. Six percent of survey respondents said Zotob's impact on their company was moderate to major, which was defined as more than $10,000 in losses and at least one major business system affected, such as e−mail or Internet connectivity. According to the study, Zotob did far less damage than did other major worms designed to exploit Windows vulnerabilities. For example, the Nimda and

MSBlast worm made a moderate to major impact on 60 percent and 30 percent of companies, respectively. Zotob was less widespread, in part, because it targeted only PCs running Windows 2000. The worm exploited a hole in the operating system's plug−and−play feature, and let attackers take control of infected machines. Twenty−six percent of Zotob victims noted that infections occurred because they had no firewall in place. The health care industry was hit hardest, with more than a quarter of that sector's organizations reporting some impact.
Cybertrust report: http://www.cybertrust.com/pr_events/2005/20051026.shtml
Source: http://news.com.com/Zotob+damage+deep+but+not+widespread/2100−7355_3−5915591.html?tag=nefd.top

20. *October 26, Security Focus* — **University of Washington IMAP mailbox name buffer overflow vulnerability.** University of Washington imap is prone to a buffer overflow vulnerability. This issue is exposed when the application parses mailbox names. Remote exploitation allows attackers to execute arbitrary code. The vulnerability specifically exists due to insufficient bounds checking on user supplied values.
Source: http://www.securityfocus.com/bid/15009/references

21. *October 26, Palm Beach Post* — **Power outages drag down phone service.** Palm Beach County, FL, experienced widespread power outages Tuesday, October 25, after a day without electricity drained backup batteries for cellular and land−line systems in the aftermath of Hurricane Wilma. Most phones were operating Monday morning, October 24, while Hurricane Wilma crossed Palm Beach County and the Treasure Coast. After the power failed, those systems ran on batteries that generally last from four to 10 hours, depending on usage. Phone service was sporadic on Tuesday, as batteries began to fail. Chuck Hamby, spokesperson for Verizon Wireless, said "It worked very well through the storm, but then with the power outages, more and more cell sites dropped out of the network." Many cellular towers have built−in generators that can power the towers for five to seven days. Most providers said Hurricane Wilma did not cause much structural damage to phone lines and towers.
Source: http://www.palmbeachpost.com/search/content/business/epaper/2005/10/26/a2d_phones_1026.html

22. *October 25, USA TODAY* — **Projected increase in spam will plague PC users.** Internet security experts are warning consumers of a wave of unwanted commercial e−mail in the weeks leading up to Thanksgiving, when the amount of spam could double as marketers try to reach holiday shoppers. The increase in spam is also due to the fact that more viruses are being spread by instant−messaging (IM) services that infect PCs and then turn them into zombies −− machines that are remotely controlled by hackers to spread spam and more viruses. According to Andrew Lochart, director of product marketing at e−mail security company Postini, attacks on IM services increased 350 percent, to 541, in the second quarter from the previous quarter. Spammers are resorting to IM attacks because consumers use software to defend PCs from e−mail−based viruses, and "there isn't much in terms of anti−virus software for IM," he says. In addition, spammers are sending more e−mail in shorter bursts to overwhelm spam defenses. Blogs have also been penetrated by spammers to create "splogs," which are fake blogs with ads. According to Blake Rhodes, CEO of blog search engine IceRocket.com, about ten percent of the blogs created each day are considered splogs.
Source: http://www.usatoday.com/tech/news/computersecurity/2005−10−25−holiday−spamalanche_x.htm

23. *October 25, Government Computer News* — **Office of Management and Budget to improve IT security next fiscal year.** The Office of Management and Budget (OMB) plans to set up several lines of business for IT security in the next fiscal year. A “line of business” is a necessary business function that typically is outside of agencies’ primary missions, such as cybersecurity. Rather than have each agency duplicate non−essential functions, OMB designates agencies with expertise in these areas to provide them to other agencies on a fee−for−service basis. Four problem areas will be addressed: (1)security training: to standardize security processes, develop common criteria, and help provide a career path for information security professionals; (2) Federal Information Security Management Act reporting: to standardize reporting processes and help ensure consistent and effective IT program management; (3) situational awareness and incident response: to improve the sharing of information about IT vulnerabilities and threats and provide resources for responding to security incidents; and (4) lifecycle security solutions: to provide a methodology for evaluating security tools. The program will not replace existing IT security programs and resources, such as the U.S.−Computer Emergency Readiness Team. According to OMB estimates, federal spending on security has been static, at about $4.2 billion a year for the last three years, while total IT spending has been slowly growing.
Source: http://www.gcn.com/vol1_no1/daily−updates/37418−1.html

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 several buffer overflow vulnerabilities in Skype that may allow a remote attacker to execute arbitrary code. The most critical of these issues can be exploited by sending a specially crafted packet to a vulnerable Skype installation. The are other two vulnerabilities which can be exploited by accessing a specially crafted VCARD or Skype URI. For more information concerning these vulnerabilities can be found in the following US−CERT Vulnerabilities Notes:

VU#905177 − For Skype vulnerable to heap based buffer overflow please see: http://www.kb.cert.org/vuls/id/905177

VU#668193 − For Skype VCARD handling routine contains a buffer overflow please see: http://www.kb.cert.org/vuls/id/668193

VU#930345 − For Skype URI handling routine contains a buffer overflow please see: http://www.kb.cert.org/vuls/id/930345

Skype has released the following Security Bulletins to address these vulnerabilities:

For input on SKYPE−SB/2005−003 please see URL: http://www.skype.com/security/skype−sb−2005−03.html

For input on SKYPE−SB/2005−002 please see URL: http://www.skype.com/security/skype−sb−2005−02.html

US−CERT recommends Skype users to upgrade to the latest fixed version of Skype as soon as possible.

Top Source Port / IP Addresses: Increased reported port activity: 1026 UDP, 1026 UDP, 1029 UDP, 1030 UDP from the following IP blocks, located in China: 221.10.254.31, 222.38.148.21, 218.27.16.180, 221.208.208.8, 221.12.161.99, 220.164.140.226, 202.103.86.66, and 222.241.95.6

US−CERT strongly recommends that all users reference the Federal Emergency Management Agency (FEMA) web site for a list of legitimate charities to donate to their charity of choice. http://www.fema.gov/

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 26777 (−−−), 135 (epmap), 40000 (−−−), 40555 (−−−), 6348 (−−−), 139 (netbios−ssn) 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.