Department of Homeland Security Daily Open Source Infrastructure Report for 25 October 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Miami Herald reports Florida Power and Light says Hurricane Wilma has left more than 2.5 million homes and businesses in South Florida without power and it could be a matter of weeks before electricity is fully restored. (See item 2)

- The Federal Emergency Management Agency has announced that federal disaster aid has been made available for Florida to help recovery efforts in the area struck by Hurricane Wilma beginning on October 23. (See item 21)

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 24, Reuters* — **Nuclear power plants shut down in response to hurricane.** Hurricane Wilma forced Florida Power and Light (FP&L) to shut three nuclear reactors in the state, company officials said Monday, October 24. FP&L has shut the 839−megawatt (MW) unit two at the St. Lucie nuclear power station and both 693 MW units at the Turkey Point nuclear power station. Nuclear power plants are robust structures built to sustain hurricane−force winds and other natural disasters but the U.S. Nuclear Regulatory Commission requires the operators to shut the plants in advance of the arrival of hurricane force winds. The 2,205 MW Turkey Point station is located in Florida City, in Miami−Dade County. The 1,678

MW St. Lucie station is located on Hutchinson Island, in St. Lucie County. There are two 839 MW units one and two at St. Lucie. The company shut unit one for a planned eight−week refueling outage over the weekend of October 15−16.
Source: http://www.alertnet.org/thenews/newsdesk/N2432725.htm

2. *October 24, Miami Herald* — **It may be weeks before power is fully restored according to utility.** Hurricane Wilma ripped through power lines and plunged more than 2.5 million homes and businesses into a darkness that could last for as long as four weeks, officials said. As of Monday night, October 24, about 954,400 customers in Miami−Dade, 862,800 in Broward and 653,700 in Palm Beach County were without electricity−−more than 95 percent of Florida Power & Light customers in those counties. Unlike past storms, Wilma knocked out key power substations and transmission lines−−crucial infrastructure that feeds electricity to smaller distribution lines and, then, to individual neighborhoods. That's why, a FPL spokesperson said, power may take so long to restore. The storm also killed power completely to the Upper and Middle Keys. By Monday afternoon 5,000 of those accounts had been restored, but some 26,000 were still without power, the Florida Keys Electricity Cooperative reported. Lingering tropical force winds delayed FPL crews from getting to work until Monday afternoon. For FPL, which has a 35−county, 27,000−square mile service area, Wilma was a record breaker. It knocked out power to 3.2 million clients, affecting more than six million people. That record was previously held by 2004's Hurricane Frances, which knocked out power to 2.7 million clients.
Florida Keys Electic Cooperative: http://www.fkec.com/
Florida Power and Light: http://www.fpl.com/
Source: http://www.miami.com/mld/miamiherald/12987508.htm

3. *October 24, Phoenix Business Journal* — **Arizona renewable energy projects picking up speed.** A quickly growing number of renewable energy projects are under way or planned in Arizona, with everyone from the federal government to local entrepreneurs leading the charge. Utilities Arizona Public Service Co. and Salt River Project each have a number of renewable energy projects up and running, with more are planned, and the U.S. Department of Agriculture (USDA) also has become intimately involved with renewable energy projects in Arizona. The USDA this week announced a $16 million loan guarantee that will help build a 20−megawatt, wood−burning electrical power plant outside of Snowflake. It is expected to be open by the end of 2006 and eventually power 20,000 homes in the White Mountains. Also, the USDA gave a $500,000 grant this week to the Gila River Indian Community for a solar power project that will provide electricity to the Sheraton Wild Horse Pass Resort and the newly relocated Rawhide theme park. The uptick in renewable energy projects can be tied both to federal and state mandates for the use of nonfossil fuels. In August, the Arizona Corporation Commission mandated that by 2025, fifteen percent of all electricity sold in Arizona must come from renewable sources.
Source: http://www.bizjournals.com/phoenix/stories/2005/10/24/story6 .html?from_rss=1

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

Nothing to report.

[Return to top]

Banking and Finance Sector

4. *October 24, U.S. Immigration and Customs Enforcement* — **Four sentenced in international money laundering investigation.** U.S. Immigration and Customs Enforcement (ICE) announced that four members of an international money laundering and narcotics organization based out of Colombia were sentenced this week for their conviction to conducting illegal financial transactions to generate money through the illegal sale and distribution of narcotics. ICE along with state, local and international partners arrested 24 individuals on October 15, 2004. The objective of the Colombian−based criminal organization was to generate money through the illegal sale and distribution of narcotics so it could be later transferred from Puerto Rico and Miami to the Colombian owners. The defendants and their co−conspirators also provided multiple bank accounts throughout the United States, Colombia, Costa Rica and China and instructions for the electronic transfer of the money to the Colombians. The investigation revealed that the organization had laundered over $4 million into 14 properties located in Colombia and 16 different international and domestic bank accounts. The four men who pleaded guilty are two Dominicans Ramon Germonsen and Victor Miliano were sentenced to 24 and 57 months in prison respectively while United States citizens Luis Torres Velazquez and Miguel Madera−Cortijo were sentenced to 120 and 46 months.
Source: http://www.ice.gov/graphics/news/newsreleases/articles/05102 4sanjuan.htm

5. *October 23, MarketWatch* — **Identity thieves target college aid money.** Financial−aid identity theft is "a growing area of concern," said Natalie Forbort, special agent in charge at the U.S. Education Department's Office of Inspector General, which investigates all types of financial−aid fraud. The crime is particularly vexing for victims, whose first indication they've been targeted may be when their own student−aid request is turned down or when they are refused another type of loan over a default they know nothing about. The increasingly electronic world of financial aid helps identity thieves stay anonymous, Fortbort said. "They're applying online for financial aid, enrolling online, they stay enrolled for 30 days and then move on," said Fortbort. Often, thieves target community colleges, where tuition is cheap, thus leaving more money to line their own pockets. Thanks to the advent of online classes, thieves can steal money "in several states because of the fact they don't physically have to be in school," Forbort said. "The schools do not want to make someone come in ... it defeats the purpose of distance education," said Fortbort.
Source: http://www.marketwatch.com/news/story.asp?guid={15689E88−632 0−4E8D−8474−764C65821751}&doctype=103

[Return to top]

Transportation and Border Security Sector

6. *October 24, Miami Herald (FL)* — **Expedited airport security lines in Orlando.** At Orlando International Airport, select passengers are having their eyes scanned or their fingerprints analyzed in order to expedite the security check process on the way to their flights. Prior to the security check, a government database has already confirmed these passengers' backgrounds, thereby allowing them to bypass the standard extra pat−down for suspicious travel patterns. Verified Identity Pass runs the Orlando service, the only ongoing test program in the Transportation Security Administration's effort to expand similar systems nationwide. With frequent fliers making up a large chunk of air travel, officials hope to ease security lines by pre−screening repeat customers and moving them through special check points. The 9,000 Verified ID customers paid about $80 for their perks in Orlando. The main benefit is a special line, where fingerprints and irises are checked (customers pick the procedure they prefer). They still must pass through a metal detector, remove their shoes as needed and take laptops out of their carrying cases for screeners. But experts expect "trusted traveler" lines to do away with those hassles too as the programs advance and screening companies pay for more advanced equipment.
Source: http://www.miami.com/mld/miamiherald/business/special_packages/business_monday/12966641.htm

7. *October 24, Associated Press* — **United Airlines pilot removed from plane.** A United Airlines pilot was removed from the cockpit Sunday, October 23, and questioned by police after security screeners at Miami International Airport reported smelling alcohol, police said. The pilot was not arrested and a breath test was not done, but the airline suspended him pending an internal investigation. The Federal Aviation Administration (FAA) is also investigating. "United's alcohol policy is among the strictest in the industry, and we have absolutely no tolerance for abuse or violation of this well−established policy," airline spokesperson Robin Urbanski said. The pilot in Sunday's incident was boarding Flight 1404 to Dulles International Airport when Transportation Security Administration screeners thought they smelled alcohol and alerted police, said FAA spokesperson Kathleen Bergen. The flight had been scheduled to leave at 9 a.m. EDT with 76 passengers. According to United's Website, it took off at 3:40 p.m. EDT after a crew change.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/10/23/AR2005102301031.html

8. *September 23, Government Accountability Office* — **GAO−05−935: Transportation Security Administration: More Clarity on the Authority of Security Directors Is Needed (Report).** The Transportation Security Administration (TSA) assigned the Federal Security Directors (FSD) to oversee security, including the screening of passengers and their baggage, at the nation's more than 440 commercial airports. FSDs must work closely with stakeholders to ensure that airports are adequately protected and prepared in the event of a terrorist attack. This report addresses (1) the roles and responsibilities of FSDs and the clarity of their authority relative to that of other airport stakeholders during security incidents, (2) the extent to which FSDs formed and facilitated partnerships with airport stakeholders, and (3) FSDs' views of key changes TSA made to better support or empower the FSD position. The Government Accountability Office (GAO) recommends that the Secretary of Homeland Security direct TSA to update its Delegation of Authority to FSDs and communicate this information to FSDs and airport stakeholders. The Department of Homeland Security generally concurred with GAO's

findings and recommendations and described corrective actions that it has initiated or plans to take to address the issues identified.
Highlights: http://www.gao.gov/highlights/d05935high.pdf
Source: http://www.gao.gov/new.items/d05935.pdf

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

9. *October 24, Reuters* — **U.S. Department of Agriculture to inspect Florida citrus crop after Hurricane Wilma.** The U.S. Department of Agriculture (USDA) will send scouts this week to check Florida's citrus groves for damage from Hurricane Wilma, which hit the state on Monday, October 24. Wilma lost strength as it raced across southern Florida near Miami−Fort Lauderdale, but it still pounded the area with heavy rain and winds as high as 125 mph. The lion's share of Florida's midseason citrus crop, 89 percent, is grown in the lower half of the state, according to the USDA. "It did cross the state pretty much south of the citrus areas," said Bob Terry, an official with the USDA's Florida Agricultural Statistics Service. "But it was such a big storm that the effects (on the citrus crop) are probably going to be pretty widespread." Terry said citrus scouts would be looking for tree damage and fallen fruit to determine the impact from Wilma. Production has already been cut this year in some parts of Florida by citrus canker disease, which causes fruit to drop prematurely. Wilma's winds could blow the contagious disease into new citrus−growing areas. Last year, three storms destroyed 40 percent of Florida's citrus crop.
Source: http://today.reuters.com/investing/financeArticle.aspx?type=bondsNews&storyID=2005−10−24T191456Z_01_N24119356_RTRIDST_0_WEATHER−WILMA−CITRUS.XML

10. *October 24, Reuters* — **Brazil's foot−and−mouth disease outbreak spreading.** An outbreak of foot−and−mouth disease has apparently spread to cattle in Parana state from neighboring Mato Grosso do Sul in Brazil, the world's top cattle producer, the federal government's agriculture minister said on Saturday, October 22. "It clearly is related to the original outbreak in Mato Grosso do Sul," Roberto Rodrigues told journalists. Investigators are examining an area near the Parana cities of Londrina and Toledo with 4,000 cattle spread across 40 ranches. "About 20 head of this total showed early signs of the illness," he said. "It's not a certainty that it is foot−and−mouth, but we are 90 percent certain that they have the disease because the group of animals came from Mato Grosso do Sul," he said. At least 41 countries have restricted imports of Brazilian beef since the first outbreak was discovered on October 10. At least 5,100 head of cattle in the region will be slaughtered in and around the region of Eldorado, Mato Grosso do Sul, Brazil's number one cattle−ranching state. But the number could climb if the quarantine area grows.
Source: http://news.yahoo.com/s/nm/20051024/hl_nm/brazil_foot_mouth_

dc;_ylt=Ah_WDgkwJhuiLJyEZ8_lHZAQ.3QA;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

11. *October 23, Lebanon Daily Record (MO)* — **Disease impacting Missouri deer population.** This year's drought conditions in Missouri have impacted the state's deer population. A viral disease is claiming some of the state's deer population, and wildlife research biologist with the Conservation Department Lonnie Hansen said Friday, October 21, it is associated with the state's dry conditions. He also said the death−rate is not as high as he expected. Hansen explained that Epizootic hemorrhagic disease (EHD) is effecting deer populations across Missouri, and has been found to be more prevalent in counties in the southwestern part of the state. Hemorrhagic disease is a viral infection that is spread through the bites of tiny flies known as midges. Conditions that concentrate deer help spread EHD by increasing the opportunity for midges to carry the virus between animals. Such conditions most often occur during dry weather in late summer and early fall, when deer gather around a few water sources. Symptoms of the disease include weakness, swelling of the mouth and tongue, sores on the mouth and tongue and bleeding from the mouth, nose, eyes, or anus. The disease causes thirst, and affected animals often die near water. Hansen said an infected animal usually dies within three days.
Source: http://www.lebanondailyrecord.com/articles/2005/10/23/local__news/news01.txt

12. *October 21, Detroit Free Press (MI)* — **Researchers: No way to halt tree−killing beetle's destruction.** The Canadian government says there's no way to stop an Asian beetle from steadily spreading to attack and kill all 10−billion ash trees in the U.S. and Canada. The emerald ash borer (EAB) was found in just three years ago in the Detroit, MI, but researchers suspect it arrived as much as a decade ago. The U.S. government has stuck with a strategy of cutting down swaths of trees to keep it from spreading, but more researchers are saying that approach will at best slow the insect. The EAB is concentrated in Michigan, northern Ohio, Indiana, and southern Ontario, Canada. Small infestations have been found in Maryland and Virginia. If it uses Ohio or Michigan's Upper Peninsula as a bridge, it could devastate dense ash forests from Minnesota to Maine. The Canadian government's official position is that the technology and efforts available cannot stop the EAB's march, a forestry official said. "It is well−established and is much too difficult to detect at low levels, and pesticides do not work well enough to be used in a quarantine context," said Ken Marchant, with the Canadian Food Inspection Service. "It is the general consensus of quarantine experts here that the EAB will continue to spread."
Multistate EAB Website: http://www.emeraldashborer.info/
Source: http://www.freep.com/news/statewire/sw122938_20051021.htm

[Return to top]

Food Sector

13. *October 24, Associated Press* — **Japan delays ending U.S. beef ban.** A Japanese government panel on mad cow disease delayed a decision Monday, October 24, on easing the ban on U.S. beef imports. This comes even though the group had prepared a draft report concluding the risk from American beef is very low. The panel had been widely expected to send the report to the Food Safety Commission, setting in motion a process that could lead to the reopening of Japan

−− U.S. beef's most lucrative overseas market −− to the imports by the end of the year. Japan imposed the ban in 2003, after mad cow disease was discovered in one animal in Washington state. Japan bought about $1.5 billion worth of U.S. beef in 2003, making it the most lucrative overseas market for American beef products. U.S. beef producers and their supporters have argued that the ban was unnecessary and have accused Japan of dragging its feet on lifting it. Yasuhiro Yoshikawa, chairman of the panel, said he hoped the panel would reach a final decision as early as at the next meeting, which is expected later this month or early next month.
Source: http://www.cbsnews.com/stories/2005/10/24/world/main966790.s html

[Return to top]

Water Sector

14. *October 22, Idaho State Journal* — **Idaho town could run out of water in next five years.** Declining aquifer water levels in southern Idaho means Twin Falls will run out of water in five years unless new drinking supplies are secured. Boise, ID, based J−U−B Engineers released the study this week that found Twin Falls' wells will decline in production because of the drought and other adverse effects on the aquifer, a pattern that has already been observed. "Twin Falls is not alone, if that's any comfort −− it's happening everywhere," said Bill Block, J−U−B senior project manager. The aquifer has declined steadily as the number of wells has increased and irrigators turn to sprinkler systems rather than flow irrigation. But aquifer levels have dropped even more because of the drought that's affected the West the past several years. The situation is further complicated by a new federal standard that reduces the amount of arsenic allowed in drinking water. The new standard becomes law in January. Half of the city's drinking water wells produce water containing arsenic levels above the 10 parts per billion the new standard allows. According to the study, the city will see a 3.5 million gallon shortfall in 2010. By 2015, the deficit will be 74.1 million gallons and by 2035 it will be 797.8 million gallons.
Source: http://www.journalnet.com/articles/2005/10/21/news/local/new s05.txt

15. *October 20, Sacramento Bee (CA)* — **Tainted water warning issued in Sacramento.** Occupants of 9,000 homes, schools, and businesses in the El Dorado Hills area of California, received contaminated tap water for about 21 hours before the problem was discovered Wednesday, October 19, and residents were warned not to drink the water. Officials with the El Dorado Irrigation District first warned nearby schools and then sent out automated phone messages advising households and businesses not to drink the water or cook or brush teeth with it for the next 48 hours. District officials said they mistakenly added coal fly ash at the El Dorado Hills water treatment plant Tuesday, October 18. Operators believed the material was soda ash, which is used to reduce acidity. After realizing the mistake, Wednesday, October 19, the district shut down the plant, switched to untainted supplies and notified state health officials and local schools. An estimated four million gallons of tainted drinking water was distributed before the problem was corrected, district officials said.
Source: http://www.sacbee.com/content/news/story/13741866p−14583805c .html

[Return to top]

Public Health Sector

16. *October 25, Nation (Thailand)* — **Bird flu virus now in 39 Thai provinces.** Avian influenza has spread to more than half of Thailand, with 39 provinces reporting confirmed or suspected cases of fresh bird−flu infections. Last week, the authorities had just 21 provinces under close watch for bird flu. Kanchanaburi, Nakhon Pathom, Nonthaburi, Suphan Buri, and Kamphaeng Phet have been put on a list of provinces with severe bird−flu problems. "We are receiving more and more reports of fowl deaths," Jatuporn Kamchuen, the livestock chief of Kanchanaburi's Phanom Thuan district, said. Livestock officials were busy culling fowl suspected of contracting bird flu. Last week, two residents of Phanom Thuan district became the latest confirmed bird−flu patients in the country. One has since died. As of Monday, October 24, three others in Kanchanaburi were on a list of people suspected of catching bird flu. Kanchanaburi public−health chief Surapong Tanthanasrikul said health volunteers were going to areas where bird−flu infections had been reported to check whether the disease had spread to any other people. In Nakhon Pathom, Pinij Hiranchote, director of the provincial hospital, disclosed that there was a suspected case of human−infection in the central province.
Source: http://nationmultimedia.com/2005/10/25/national/index.php?news=national_18960922.html

17. *October 24, Reuters* — **Pig disease killed Hong Kong man.** A Hong Kong man who died in hospital earlier this month had the pig−borne disease Streptococcus suis, the territory's government said on Monday, October 24, citing lab tests. The man was the 12th person from Hong Kong to be infected with the disease this year, the government said in a statement. The disease has killed around 40 people in mainland China. The 43−year−old, who had no recent travel history, was admitted to hospital on October 13. He died on the same day and his family was placed under medical observation, it said. Most of the more than 200 people reported to have caught the disease on the mainland became sick after slaughtering, handling, or eating infected pigs.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2005−10−24T142123Z_01_RID451646_RTRIDST_0_HEALTH−HK−PIG−DISEASE−DC.XML&archived=False

18. *October 24, Agence France−Presse* — **United Nations' food agency to send bird flu experts to Indonesia.** The United Nations' Food and Agriculture Organization (FAO) is to send a team of experts to Indonesia to help fight an outbreak of avian flu in that country. Joseph Domenech, the head of the FAO's veterinary service, said the aim was to help Indonesia combat the virus at source, by organizing a house−by−house search for infected birds. Indonesia has so far confirmed the deaths of three humans from bird flu. Domenech said the first priority for the project, which was being financed by the U.S. Agency for International Development (USAID), would be combating the virus on Indonesia's most populated island, Java.
Source: http://www.thejakartapost.com/detaillatestnews.asp?fileid=20 051024190807&irec=1

19. *October 24, Department of Homeland Security* — **EPA and DHS announce new Center of Excellence for Research on microbial risk assessment for Homeland Security.** The Department of Homeland Security (DHS) and the Environmental Protection Agency (EPA) on Monday, October 24, announced the establishment of a jointly funded research center based at Michigan State University that will fill critical gaps in microbial risk assessment needed to support homeland security objectives. One grant of $10 million for five years was awarded to

establish the center. The new research center, named the Center for Advancing Microbial Risk Assessment (CAMRA), will provide policy−makers and first responders with the information they need to protect human life from biological threats and to set decontamination goals by focusing on two primary objectives. The first objective is a technical mission to develop models, tools, and information that can be used to reduce or eliminate health impacts from the deliberate indoor or outdoor use of biological agents. The second objective is a knowledge management mission to build a national network for information transfer about microbial risk assessment among universities, professionals, and communities. The scientists involved have extensive expertise in microbial risk assessment methods, biosecurity, and infectious disease transmission through environmental exposure. The CAMRA schools include Michigan State University, Carnegie Mellon University, Drexel University, Northern Arizona University, University of Arizona, University of California at Berkeley, and the University of Michigan
Source: http://www.dhs.gov/dhspublic/display?content=4902

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

20. *October 24, Union−Tribune (CA)* — **Airport Authority stages emergency drill at Lindbergh Field.** There was a smoking jetliner off the side of a runway at Lindbergh Field surrounded by emergency vehicles Monday, October 24, there's no cause for alarm. A major emergency drill took place as several agencies test their preparedness skills in responding to an airport disaster, according to the San Diego County Regional Airport Authority, which was leading the full−scale emergency exercise. The exercise involved the simulation of jetliner −− dubbed Air Ex 2005 −− that has experienced a landing problem. The emergency scenario has the jet veering off the runway and catching fire. The drills are designed to test the capabilities of airport and airline personnel and the agencies responsible for responding in a disaster. The FAA, the Transportation Security Administration, the Red Cross and HOPE Animal−Assisted Crisis Response teams also were involved in the drill.
Source: http://www.signonsandiego.com/news/metro/20051024−0924−bn24d rill.html

21. *October 24, Federal Emergency Management Agency* — **FEMA: President declares major disaster for Florida.** Acting Director R. David Paulison of the Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Monday, October 24, that federal disaster aid has been made available for Florida to help recovery efforts in the area struck by Hurricane Wilma beginning on October 23, 2005, and continuing. Paulison, said the assistance was authorized under a major disaster declaration issued for the state by President Bush, and designated the following counties eligible for aid to stricken residents and business owners: Collier, Lee, and Monroe Counties. The assistance, to be coordinated by FEMA, can include grants to help pay for temporary housing, home repairs and other serious disaster−related expenses. Low−interest loans from the U.S. Small Business Administration

also will be available to cover residential and business losses not fully compensated by insurance. Paulison indicated that more counties and additional forms of assistance may be designated after assessments are fully completed in the affected areas. He named Justin DeMello as the Federal Coordinating Officer for Federal recovery operations in the affected areas.
Source: http://www.fema.gov/news/newsrelease.fema?id=20006

[Return to top]

Information Technology and Telecommunications Sector

22. *October 23, New York Times* — **Colleges protest call to upgrade online systems.** The Federal Communications Commission is requiring hundreds of universities, online communications companies and cities to overhaul their Internet computer networks to make it easier for law enforcement authorities to monitor e−mail and other online communications. This order extends the provisions of a 1994 wiretap law to universities, libraries, airports providing wireless service and commercial Internet access providers and municipalities that provide Internet access to residents, such as Philadelphia and San Francisco. The action, which the government says is intended to help catch terrorists and other criminals, has unleashed protests and the threat of lawsuits from universities, which argue that it will cost them at least $7 billion while doing little to apprehend lawbreakers. The Justice Department requested the order last year, saying that new technologies like telephone service over the Internet were endangering law enforcement's ability to conduct wiretaps "in their fight against criminals, terrorists and spies."
Source: http://www.nytimes.com/2005/10/23/technology/23college.html

23. *October 22, Open Source Vulnerability Database* — **RSA authentication agent for Web IISWebAgentIF.dll redirect overflow vulnerability.** A remote overflow exists in RSA authentication agent for Web for IIS. IISWebAgentIF.dll fails to validate the length of the "url" parameter in the "Redirect" method, resulting in a stack−based buffer overflow. With a specially crafted GET request, an attacker can cause arbitrary code execution resulting in a loss of integrity. RSA Authentication Agent for Web for IIS is an ISAPI filter which runs in−process with inetinfo.exe. Any attempt to exploit this flaw will result in the termination and potential restart of the IIS service. Currently, there are no known workarounds or upgrades to correct this issue. However, RSA Security has reportedly released a patch to address this vulnerability.
RSA Security: http://rsasecurity.com/
Source: http://www.osvdb.org/displayvuln.php?osvdb_id=20151

24. *October 22, Open Source Vulnerability Database* — **CA iGateway debug mode HTTP GET request overflow vulnerability.** A remote overflow exists in Computer Associates iGateway. The application fails to perform proper bounds checking resulting in a buffer overflow. With a specially crafted HTTP GET request, a remote attacker can cause arbitrary code execution with SYSTEM privileges resulting in a loss of integrity. This flaw is only exploitable if a non−standard installation has been performed and when the iGateway component has been explicitly configured to run with diagnostic debug tracing enabled. The vulnerability can be fixed with an upgrade to version 4.0.050623 or higher, as recommended by Computer

Associates. An upgrade is required as there are no known workarounds.
Vendor Specific Advisory URL:
http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=334 85
Source: http://www.osvdb.org/displayvuln.php?osvdb_id=19920

25. *October 22, Open Source Vulnerability Database* — **Sophos anti−virus visio file processing overflow vulnerability.** A remote overflow exists in Sophos anti−virus in which the anti−virus engine fails to perform proper bounds checking, which results in a heap−based buffer overflow. With a specially crafted visio file, a remote attacker can cause arbitrary code execution resulting in a loss of integrity. According to OSVDB, the vendor should be contacted for an appropriate upgrade. An upgrade is required as there are no known workarounds.
Vendor Specific Advisory URL:
http://www.sophos.com/support/knowledgebase/article/3409.htm l
Source: http://www.osvdb.org/displayvuln.php?osvdb_id=18464

26. *October 21, IDG News Service* — **Microsoft reports second patch problem; Windows 2000 users may be unprotected.** A critical patch – Security Update MS05−050 – released by Microsoft on October 11 as part of the company's monthly security software fixes related to Microsoft's DirectShow streaming media software may have left users vulnerable. Microsoft DirectX 8.0 or 9.0 users who may have accidentally installed the patch written for DirectX 7.0 will still be vulnerable to the underlying vulnerability. The patch is supposed to address a problem in DirectShow that could allow an attacker to seize control of an unpatched system. According to Microsoft, customers who received Update MS05−050 automatically or who correctly followed the steps in Microsoft's security bulletin won't be affected. Another patch released on October 11 – MS05−051 – gave users difficulties as well.
Microsoft Security Bulletin: http://www.microsoft.com/technet/security/bulletin/ms05−oct.mspx
Source: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,105646,00.html

27. *October 20, InformationWeek* — **Hackers, scammers hid malicious javascript on Websites.** Internet thieves are using a new, fast spreading technique called "JS/Wonka" to conceal their code. The JS/Wonka technique converts characters to and from their respective Unicode values. JavaScript completes those conversions automatically, so it doesn't require much expertise on the part of the code writer. Dan Hubbard, senior director of security and research at Websense, said, "For whatever reason, the number has just skyrocketed since the last of September…There are 10,000 unique sites using this exact same method. The strange thing is, they're completely different types of sites." Internet Explorer and Firefox, among other browsers, are vulnerable. According to Websense, three out of four of the sites found using JS/Wonka are hosted in the U.S. which is another indication that either a group of scammers is working together, or that a obfuscation toolkit has just been made available, and hasn't had time to spread overseas.
Websense's JS/Wonka Alert: http://www.websensesecuritylabs.com/resource/pdf/wslabs_wonka_analysis_oct05.pdf
Source: http://informationweek.com/story/showArticle.jhtml?articleID =172302840

28. *October 19, Vnunet* — **Rootkit creators turn professional.** Security experts are reporting a surge in the level of professionalism and commercialization in the creation of rootkits, a tool

that helps worm authors slip past malware detection tools. Antivirus vendor F−Secure has reported that it has detected a new rootkit designed to bypass detection by most of the modern rootkit detection engines. Traditionally a rootkit would be designed to evade only one security product, such as Symantec's or F−Secure's antivirus scanners. Allen Schimel, chief strategy officer at StillSecure, a developer of intrusion detection, vulnerability management, and network access control applications, says "These rootkits just cranked it up a notch in their ability to evade multiple antivirus products." Schimel also warns that if these tools are effective in penetrating a computer’s defenses, more worm authors are likely to start using them. The version of the rootkit detected by F−Secure is called Golden Hacker Defender.
Source: http://www.vnunet.com/vnunet/news/2144149/rootkits−turn−prof essional

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 reports a vulnerability in the Snort Back Orifice Parsing Remote Code Execution the exploit is in Snort’s Back Orifice pre−processor. A stack based overflow can be triggered with a single UDP packet, allowing an attacker to fully compromise a Snort or Sourcefire installation. X−Force believes this vulnerability to be trivially exploitable, and urges affected users to upgrade immediately. Snort is a widely deployed, open source network intrusion detection system (IDS). Snort and its components are used in other IDS products, notably Sourcefire Intrusion Sensors, and Snort is included with a number of operating system distributions.

Snort preprocessors are modular plugins that extend functionality by operating on packets before the detection engine is run. The Back Orifice preprocessor decodes packets to determine if they contain Back Orifice ping messages. The ping detection code does not adequately limit the amount of data that is read from the packet into a fixed length buffer, thus creating the potential for a buffer overflow. The vulnerable code will process any UDP packet that is not destined to or sourced from the default Back Orifice port (31337/udp). An attacker could exploit this vulnerability by sending a specially crafted UDP packet to a host or network monitored by Snort. US−CERT is tracking this vulnerability as VU#175500:
http://www.kb.cert.org/vuls/id/175500

A new botnet – Mocbot – is making the rounds, according to F−Secure. This botnet client has been spread using the MS05−047 vulnerability. The vulnerability can be exploited via 139/TCP and 445/TCP. The existence of a file called wudpcom.exe in the SYSTEM directory is a symptom of an infection. The botnet client tries to connect to two IRC servers in Russia, but the servers seem to be down (or overloaded). This is a heads up since botnet owners are using it to further exploit networks they already have a presence on. If you haven't already patched − you may

want to do so now:
http://www.f−secure.com/v−descs/mocbot.shtml
http://www.f−secure.com/weblog/archives/archive−102005.h tml#00000685

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 12346 (FatBitchtrojan), 135 (epmap), 139 (netbios−ssn), 4495 (−−−), 40000 (−−−), 2234 (directplay) 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

29. *October 24, Associated Press* — **State finds no dangers after emergency dam inspections.** Massachusetts Governor Romney was briefed Monday, October 24, on the results of emergency dam inspections around the state. Romney called for the reviews of 186 so−called "high hazard" dams last week, after a state of emergency was issued in Taunton, MA, over fears that the 173−year−old Whittenton Pond Dam would collapse and flood a large portion of the city. A state environmental affairs official says the inspections did not reveal any situations as dangerous as the one that existed in Taunton. The old wooden dam was dismantled over the weekend and replaced by a new structure built of rock.
Source: http://www.abc6.com/engine.pl?station=wlne&id=17687&template =breakout_story_local_news.shtml&dateformat=%25M+%25e,%25Y

[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.