Department of Homeland Security Daily Open Source Infrastructure Report for 22 May 2006

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

Daily Highlights

- The Associated Press reports the U.S.'s busiest border crossing reopened early Friday, May 19, following a nine−hour closure after federal authorities shot and killed the driver of a sport utility vehicle headed back to Mexico with what appeared to be a group of illegal immigrants. (See item 12)
- WKMG TV6 reports law enforcement and authorities at government buildings are being warned to be on the lookout for guns disguised as cell phones that are difficult to spot in metal detectors. (See item 27)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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. *May 18, Associated Press* — **Xcel takes outage blame for February outage.** Xcel Energy's CEO on Wednesday, May 17, said the utility accepts the blame for the rolling blackouts in February that cut power to roughly 300,000 customers on one of the winter's coldest days. Richard Kelly said the utility didn't realize how cold it would get on February 18 and underestimated natural gas demand when supply was constrained. About 3,000 megawatts of power −− mostly generated from natural gas and by private power producers −− went offline that day, forcing Xcel to cut power to thousands of customers for three 30−minute periods in

the morning. Kelly said Xcel didn't call the National Center for Atmospheric Research (NCAR) in Boulder to get a forecast that day. Instead, Xcel depended on other sources and internal forecasts that proved inaccurate. Xcel spokesperson Ethnie Groves later clarified that Xcel doesn't use NCAR forecasts. When asked why Xcel didn't request power from Tri−State Generation and Transmission, a wholesale supplier of power to rural electric systems, Kelly said Tri−State couldn't have responded quickly enough to prevent the outages. Tri−State has said it could have run additional power plants if Xcel had requested. State regulators are investigating to see whether things could have been done differently.
Source: http://www.rockymountainnews.com/drmn/energy/article/0,2777,DRMN_23914_4707620,00.html

2. *May 18, Utility Automation & Engineering* — **Report looks at restoration practices among utilities.** Macrosoft Inc. released the results of a survey it conducted to study the restoration practices of utility companies in North America. The report, aimed at benefiting utility companies to understand common best practices and pain points which can be effectively addressed, is the outcome of a detailed study conducted during the period of February to March 2006. The results are based on responses from over 100 storm center personnel across 45 utilities. The report highlights the importance of standardizing operations and leveraging technology to enhance efficiencies in the quick assembling of resources, their effective deployment, tracking and managing them before, during, and after the event. Some findings that emerged from the survey include: 87 percent indicated they have at least one major outage every year. Utilities in the Mid−Atlantic, Midwest and Northeast indicated they face the highest frequency of emergencies outages in excess of five major events annually. Fifty−three percent reported having over 500 field personnel deployed during a large scale restoration event. Despite available technology, a majority of companies do not use automated systems, but still use manual spreadsheets, white boards, or forms to track and manage people and equipment resources during and emergency outage.
Report (user log−in required): http://www.macrosoftinc.com/press_051606.html
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=255465&p=22

3. *May 18, Reuters* — **FERC: Electricity supplies tight in California, Connecticut.** Tight electricity supplies and growing demand could bring rolling blackouts to Southern California this summer if power plant outages deplete the grid during a heat wave, Federal Energy Regulatory Commission (FERC) staff said on Thursday, May 18 in its annual assessment of supply and demand. Southwest Connecticut also faces a dearth of supplies this summer, especially if a heat wave washes over the Northeast U.S. and limits Connecticut's ability to import power from adjoining states. Supplies will also be tight this summer in Ontario, Canada, with a possible ripple effect into the U.S. Northeast and New England states. Long Island and New York City will see tight supplies as well. With sustained heat and unexpected shut downs of local power plants, California's grid operator "might need to shed load through rolling blackouts in Southern California this summer," said Steve Harvey in FERC's office of enforcement. Rolling blackouts are "fairly unlikely" this summer, and the disastrous combination of high temperatures and plant failures is "as great in Southern California as anywhere," Harvey said. Overall U.S. power supplies are stronger than a year ago because of hydroelectric supplies in the Pacific Northwest are abundant, and coal supplies show signs of building.
Report: http://www.ferc.gov/EventCalendar/Files/20060518103507−A−3−w

ith−talking−ptsl.pdf
Source: http://today.reuters.com/investing/financeArticle.aspx?type=bondsNews&storyID=2006−05−18T170124Z_01_N18210117_RTRIDST_0_UTILITIES−FERC−SUMMER.XML

4. *May 18, U.S. Department of Energy* — **DOE Secretary Bodman tours refinery and calls for more domestic refining capacity.** Secretary of Energy Samuel W. Bodman has renewed the call for expanded oil refining capacity in the U.S. and discussed additional steps the Department of Energy (DOE) is taking to prepare for the upcoming hurricane season. Secretary Bodman made the statements after touring the Motiva Refinery in Port Arthur, Texas. He discussed a new DOE−sponsored weather modeling system and improvements to the department's Visualization Room. These upgrades will provide better−time information and forecasts, which will allow for better planning and response during a natural disaster. In January, DOE hosted a conference in Mississippi to bring together federal, state, and local governments, as well as industry leaders, to share lessons learned and best practices from the 2005 hurricane season. The department has worked with states to help them improve their energy assurance plans and will implement a toll−free hotline, which will allow state and local governments and representatives from the energy industry to improve communications with the DOE during an emergency. DOE has also increased the number of infrastructure experts capable of deployment to a region if necessary.
Source: http://www.energy.gov/news/3657.htm

[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

5. *May 29, BusinessWeek* — **Cybercrime hackers.** Dimitry Ivanovich Golubov was arrested last July for his involvement in credit card fraud and U.S. law enforcement officials hailed it as a big break in their fight against cybercrime. Subsequently, in January 2006, the U.S. Attorney's office charged Golubov with a number of cybercrimes, including credit card fraud. U.S. Postal Inspection Service senior investigator Gregory S. Crabb, who worked with Ukrainian authorities on their case, says Golubov and others controlled the numbers, names, and security codes attached to credit cards. Low−level criminals would use that to load up fake cards and withdraw cash from automated teller machines or buy merchandise. But last December, Golubov's story took a bizarre twist. Two Ukrainian politicians vouched for Golubov's character in court, and the judge released Golubov. "Chat from the carding community"

indicates Golubov may be back in business, says Crabb. His story portrays a picture of organized gangs of young, mostly Eastern European hackers who are growing more brazen about doing business on the Web. They meet in underground forums with names like DarkMarket.org and theftservices.com to trade tips and data and coordinate scams that span the globe.
Source: http://www.businessweek.com/magazine/content/06_22/b3986093. htm

6. *May 19, Associated Press* — **Four Russians detained in alleged U.S.−linked ATM theft scheme.** Four Russians have been detained on suspicion of forging bank cards and using them to steal some $500,000 from U.S. bank accounts at ATMs in Moscow, Russian police and media reports said. Police believe the suspects were working with accomplices in the United States −− possibly bank employees −− who provided them with card and PIN numbers they used to make the fake cards in an apartment in Moscow, Moscow police spokeserson Yulia Volk said Thursday, May 18. More than 100 forged cards and $60,000 were found in the apartment, she said, as well as a database with information about accounts in the United States, Canada, and France. Volk said the actual sum could be higher than $500,000. U.S. law enforcement agencies informed Russian police that money was being stolen at Moscow automated teller machines from bank accounts of Americans who had never been to Russia. Police were able to pinpoint the suspects fairly quickly because they repeatedly withdrew money at the same 10 ATMs in Moscow, always doing so at night to avoid suspicion about forged cards that lacked colorful designs. The suspects sent a portion of their take to their U.S. accomplices through Internet payment systems, Kommersant reported.
Source: http://biz.yahoo.com/ap/060519/russia_atm_theft.html?.v=1

7. *May 18, Toronto Star (Canada)* — **Canadian counterfeit ring halted by police.** At least 30 people have been arrested in the dismantling of a major counterfeit money−making ring that laundered millions of dollars of cash through popular consumer retail chains throughout Ontario and in Montreal. More than $4.5 million in counterfeit currency has been directly linked to the organization, whose members are also alleged to be responsible for a series of violent bank robberies as well as the illegal manufacturing of credit cards and the theft of credit card data. "Had this group not been stopped they would have had a significant effect on the Canadian economy," said Sgt. Moshe Gordon, a counterfeit coordinator for the RCMP. More than 10,000 debit and credit card numbers were discovered inside the hard drives of seized computers −− data that had been allegedly stolen from unsuspecting consumers since early 2005. Altogether, 469 charges have been laid so far in the investigation.
Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1147902616098&call_pageid=970599119419

8. *May 18, Websense Security Labs* — **Phishing Alert: Michigan Schools & Government Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Michigan Schools & Government Credit Union. Users receive a spoofed e−mail message, which claims that they have been randomly selected and must verify their account information. This e−mail message contains a link to a phishing Website that prompts users to enter confidential information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =491

9.

May 18, Websense Security Labs — **Phishing Alert: Premier America Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Premier America Credit Union. Users receive a spoofed e−mail message claiming that they must confirm their account information. This e−mail message contains a link to a phishing Website that prompts users to enter confidential information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =492

10. *May 18, Harris Interactive* — **Report: Substantial numbers of U.S. adults taking steps to prevent identity theft.** A recent Wall Street Journal Online/Harris Interactive Personal Finance Poll reveals that while relatively few U.S. adults say they have fallen victim to identity theft, substantial numbers have taken specific steps to help prevent it from happening to them. Three in five (60 percent) adults who have had their identity stolen lost money as a result, and while a majority recovered their losses within three months (57 percent), one in five (21 percent) say they have not yet been able to recover their loss. The poll further explores how much adults trust banks, credit card companies, insurance companies, brokers, and retailers to prevent others from accessing their sensitive personal information and account numbers, and what they do when they receive a suspicious email from a financial institution or other company with whom they have an account. Banks have been most successful in gaining public trust, as 80 percent of adults say they trust banks a fair amount or a great deal to prevent others from accessing their sensitive personal information or account number.
Report: http://www.harrisinteractive.com/news/allnewsbydate.asp?News ID=1058
Source: http://www.harrisinteractive.com/news/allnewsbydate.asp?News ID=1058

[Return to top]

Transportation and Border Security Sector

11. *May 19, USA TODAY* — **Fliers could keep their shoes on if new airport scanner is approved.** A government lab is testing a "very promising" new machine that would allow airline passengers to keep their shoes on while going through security checkpoints, the nation's aviation security chief said Thursday, May 18. The machine, which detects explosive material on shoes when people stand on a platform, is getting a "highly expedited" review at the lab, said Kip Hawley, head of the Transportation Security Administration. He wouldn't give a timetable for deploying the machines since they must pass testing in an airport before they are used to screen passengers. The ShoeScanner uses technology similar to a medical MRI to detect explosives in five to eight seconds. It shoots radio waves at shoes to agitate molecules and analyze their structure. Readings are sent to a computer that holds a library of explosives characteristics and makes a rapid comparison. Removing shoes at checkpoints has been one of the biggest inconveniences for passengers in the wake of the 9/11 terrorist attacks.
Source: http://www.usatoday.com/travel/flights/2006−05−18−shoe−scann er_x.htm

12. *May 19, Associated Press* — **San Diego border reopens after shooting.** The country's busiest border crossing reopened early Friday, May 19, following a nine−hour closure after federal authorities shot and killed the driver of a sport utility vehicle headed for Mexico, officials said. Border agents had pulled over the SUV after reports that the driver had picked up what appeared to be a group of illegal immigrants. When the driver tried to veer back into traffic on Interstate 5 Thursday afternoon, May 18, the officers fired. The Mexican government asked its

consulate to investigate the shooting, which occurred about 50 feet north of the San Ysidro Port of Entry between Tijuana, Mexico, and San Diego. Mexican presidential spokesperson Ruben Aguilar said it appeared the driver was engaging in organized crime or people smuggling and that the vehicle was trying to escape U.S. officials by crossing into Mexico. It was unclear whether Mexican citizens were involved, he said. Five people who had been in the SUV were taken into U.S. custody. U.S. Customs and Border Protection agents began following the black SUV after somebody reported seeing it pick up suspected illegal immigrants near the U.S. side of the Otay Mesa border crossing, said Lt. Kevin Rooney of San Diego Police Department.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/n/a/2006/05/19/nati onal/a061014D66.DTL

13. *May 19, Seattle Times* — **Captain arrested on suspicion of being drunk aboard cruise ship.** The captain of a 1,816−passenger cruise ship destined for Alaska was arrested at Pier 66 in Seattle on Friday, May 19, after the Coast Guard determined his blood−alcohol content was more than twice the federal maritime limit, officials said. Coast Guard Captain Steve Metruck said it's the first time in 24 years a cruise−ship captain has been arrested in the Puget Sound region on suspicion of such an offense. The man, who was preparing the ship to leave, was arrested, fired by Celebrity Cruises and immediately replaced by another captain before the ship Mercury set sail, Metruck said. "The captain's actions are totally unacceptable. He has been stripped of his command and ordered off the ship," Dan Hanrahan, president of Celebrity Cruises, said in a release. A Coast Guard inspector was aboard the Mercury to follow up on a previous safety violation involving a lifeboat lift, Metruck said, when the inspector smelled alcohol on the captain's breath and notified staff at Coast Guard headquarters.
Source: http://seattletimes.nwsource.com/html/localnews/2003007115_w ebcruise19m.html

14. *May 18, Associated Press* — **New Atlanta runway could cut delays across U.S.** Because of a new 9,000−foot runway scheduled to open in Atlanta's Hartsfield−Jackson airport on May 27, the airport's officials are pledging to cut delays in half, which also could mean fewer and shorter delays throughout the entire air transportation network in the United States and possibly around the world. That's because no other airport in the world handles more passengers. Nearly 86 million people pass through the Atlanta airport each year on more than 980,000 flights −− one taking off or landing about every 30 seconds. They fly direct to 157 cities in the U.S. and 65 others in 43 different countries. The airport's new fifth runway and a new runway monitor system will help it bring in three different streams of planes at the same time, even during foul weather. The reduced delays should reduce operating costs for airlines by an estimated total of $5 million a week, said Ben DeCosta, the airport's general manager. The airline set to benefit the most is Delta Air Lines, which uses the airport as its primary hub and is looking for any savings it can get as it works to pull out of bankruptcy.
Source: http://www.cnn.com/2006/TRAVEL/05/18/airport.runway.ap/index .html

[Return to top]

Postal and Shipping Sector

15. *May 19, DMNews* — **UPS ends cap on air fuel surcharge.** High fuel prices prompted UPS Inc., the world's largest package delivery company, to remove a cap on the surcharge added to air shipments. The Atlanta company said this week that it would remove its 12.5 percent cap on the UPS air and international small package fuel surcharge June 5. The company also will

recalibrate its air and international fuel surcharge index downward by two percentage points so that customers aren't hit with the full effect. The change reflects the rise of fuel prices to unprecedented levels and continuing volatility in the market, UPS said. Since October, the price of crude oil has risen more than 21 percent, the company said.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3698 0

[Return to top]

Agriculture Sector

16. *May 19, USAgNet* — **Equine herpes suspected on shore.** Maryland's horse racing industry received more bad news Thursday, May 18, as the equine herpes virus apparently spread to the Eastern Shore −− perhaps from a strain of the disease that arrived from Florida −− and a lack of available horses forced Laurel Park to cancel Sunday racing for the next two weeks.
Source: http://www.usagnet.com/story−national.cfm?Id=950&yr=2006

[Return to top]

Food Sector

17. *May 19, United Press International* — **Japan moves to resume U.S. beef imports.** Japan will decide whether to lift its ban on U.S. beef imports in June after it confirms there are no major problems at U.S. beef exporters' facilities. At a three−day meeting that ended Friday, May 19, in Tokyo, Japanese experts said that U.S. meat processing facilities are prepared to meet the conditions for Japan to resume importing U.S. beef, the Mainichi Shimbun reported. U.S. beef will reappear on Japanese store shelves in July at the earliest, as inspections will take several weeks, the officials said. Imports of U.S. beef were banned by Japan in December 2003, following the discovery of cows infected with mad cow disease. Japan partially lifted the ban in December 2005, but resumed it just one month later after part of a backbone was discovered in a veal shipment.
Source: http://www.market−day.net/article_3673/20060519/Japan−moves−to−resume−US−beef−imports.php

18. *May 19, Animal and Plant Health Inspection Service* — **Importation of peppers from the Republic of Korea allowed.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service on Friday, May 19, announced that it has amended the fruits and vegetables regulations to allow, under certain conditions, the importation of peppers into the continental U.S. from the Republic of Korea. Based on the scientific evidence of a recent pest risk analysis, peppers can be safely imported from the Republic of Korea, provided certain conditions are met. These requirements will continue to protect the U.S. against introductions of plant pests and diseases such as Agrotis segetum, a moth that feeds on a range of host plants, including peppers. As a condition of entry, the peppers must be grown in the Republic of Korea in approved insect−proof, pest−free greenhouses and packed in pest exclusionary packinghouses. In order to safeguard against pest infestation during their movement, the peppers must be protected by an insect−proof mesh screen or plastic tarpaulin and packed in insect−proof containers.

Source: http://www.aphis.usda.gov/newsroom/content/2006/05/kopepper. shtml

19. *May 18, Animal and Plant Health Inspection Service* — **Regulations regarding the importation of animals and animal products from the European Union amended.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is amending its regulations regarding the importation of animals and animal products into the U.S. from a region of the European Union (EU). This final rule will apply a uniform set of import requirements for classical swine fever (CSF) to the region consisting of the 15 member states that comprised the EU prior to its expansion on May 1, 2004. These member states (EU−15) are: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Italy, Luxembourg, the Netherlands, Portugal, the Republic of Ireland, Spain, Sweden and the United Kingdom. According to this final rule, import prohibitions will be placed on all swine and swine products entering the U.S. from any region in any member state of the EU−15 that has been quarantined by the EU due to an outbreak of CSF.
Source: http://www.aphis.usda.gov/newsroom/content/2006/05/eu15csf.s html

20. *May 18, U.S. Food and Drug Administration* — **Cheese recalled.** Swiss−American, Inc. of St. Louis, MO, is recalling cut pieces of Cut Cahill's Farm Porter Cheese, because Listeria monocytogenes was discovered in sampled product. Listeria monocytogenes is an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Cut Cahill's Farm Porter Cheese was distributed primarily through retail grocery stores in Missouri and Illinois. Product was also distributed to two stores in Louisiana and Tennessee. All product from Louisiana has been recovered. No illnesses have been reported to date. Swiss−American was informed that Listeria monocytogenes was found in the imported bulk product as part of routine testing procedures.
Source: http://www.fda.gov/oc/po/firmrecalls/swissamerican05_06.html

[Return to top]

Water Sector

21. *May 19, Los Angeles Times* — **Water suppliers warned to submit safety reports.** The U.S. Environmental Protection Agency (EPA) has issued warnings to 18 small drinking water suppliers in California, saying they could be fined for failing to submit plans describing how they would prevent or respond to terrorist attacks. The cities of Perris and Norco and the Lake Arrowhead Community Service District were among water suppliers that submitted no plans for emergency response or reducing vulnerability to terrorism, which were due in 2004. The city of San Jacinto did not provide an emergency response plan. If suppliers without vulnerability plans do not submit them within a month, the companies could face up to $32,000 a day in court−ordered penalties, EPA officials said. Federal legislation in 2002 ordered all water systems that serve more than 3,300 customers to submit plans.
Source: http://www.latimes.com/news/printedition/california/la−me−ie briefs19may19,1,125695.story?coll=la−headlines−pe−california

22. *May 18, Xinhua (China)* — **Toxic chemical containers missing in river, water supply to 60,000 people affected.** Two barrels of toxic chemicals missing in a river in northwest China's

Gansu Province, after an upriver traffic accident on Sunday, May 14, has affected the water supply of 60,000 people, official sources said on Thursday, May 18. A truck carrying ten barrels of TDI overturned in the county of Jiuzhaigou on the southern border with Sichuan Province dumping all the containers into the adjacent Tangzhu River, which joins the trunk stream of Baishui River and flows northward into Wenxian County of Gansu, the environmental protection bureau of Wenxian said. The Sichuan government informed Gansu of the accident in time and Wenxian immediately suspended the water supply from the river. Eight barrels have been retrieved. TDI, a toluene−like chemical usually used as an ingredient of industrial paint, is harmful to people's respiration system, eyes and skin. About 60,000 residents living along the river section in the county have turned to mountain springs for the past four days, but the water supply to the rest of the population was not affected.
Source: http://news.xinhuanet.com/english/2006−05/18/content_4569109 .htm

[Return to top]

Public Health Sector

23. *May 19, Agence France−Presse* — **Four arrested in Romania for spreading bird flu.** The manager of a major industrial poultry farm in Romania has been arrested on charges of allowing the farm to sell chickens possibly infected with a potentially lethal form of bird flu, prosecutors in the town of Brasov said. The unnamed manager is the third person from the Drakom Silva poultry operation in Codlea to be arrested in the last few days. The farm's veterinarian and its owner were both arrested on Wednesday, May 17, as was the owner of another poultry farm in the town.
Source: http://www.breitbart.com/news/2006/05/19/060519110204.4jdyfb n4.html

24. *May 19, Agence France−Presse* — **Denmark confirms H5N1 bird flu in domestic poultry.** Danish authorities have confirmed the country's first case of the H5N1 strain of bird flu in domestic birds. This is the first reported case of H5N1 in tame poultry in the Scandinavian country. The country has reported 47 cases of the H5N1 strain of bird flu in wild birds since March. The authorities reported on Thursday, May 18, finding the H5 family of bird flu in two chickens and a peacock in the private farm in Hundslev, near Kerteminde on Fyn Island, central Denmark.
Source: http://news.yahoo.com/s/afp/20060519/hl_afp/healthfludenmark_060519111134;_ylt=AnoLOHvtNhPS._.73wmdANiJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

25. *May 19, Agence France−Presse* — **Polio strikes Democratic Republic of Congo.** Polio has returned to the Democratic Republic of Congo (DRC) for the first time in six years, the World Health Organization (WHO) announced on Friday, May 19. WHO spokesperson Fadela Chaib told reporters that a two−and−a−half year old girl had been paralyzed by a strain of the polio virus that had been carried from India via Angola. WHO was planning a vaccination campaign in the child's home−region near the Angolan border to stifle the spread of a virus, she said.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.mg.co.za/articlepage.aspx?area=/breaking_news/breaking_news__africa/&articleid=272230

26. *May 18, Agence France−Presse* — **Cases of H5N1 bird flu found in Siberia.** Russian veterinary services said they had found new cases of the H5N1 strain of bird flu near Omsk in Siberia. Confirming that "a few birds" in the region had the disease, Nikolai Vlassov, deputy head of the veterinary services, said that two villages in the area had been placed under quarantine.
Source: http://news.yahoo.com/s/afp/20060518/hl_afp/healthflurussia_060518201208;_ylt=Aq2zZ75WSer4y2pst7pkRlyJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

27. *May 19, WKMG TV6 (FL)* — **New cell phone guns hard to spot in metal detectors.** Law enforcement and authorities at government buildings are being warned to be on the lookout for guns disguised as cell phones that are difficult to spot in metal detectors, according to a Local 6 News report. The report said the cell phone gun is a working .22 caliber pistol capable of firing off four rounds at the touch of the button. The hidden guns are made of high−grade plastic, which makes them difficult to spot in metal detectors, the report said. NYPD officers are also being told to be on the lookout for the custom−made guns. The cell guns are considered illegal to possess because they are not made by a licensed gun manufacturer. Federal firearms agents said cell phone guns are only the latest in a long line of seemingly harmless but lethal weapons including belt buckle guns.
Source: http://www.local6.com/news/9243672/detail.html

[Return to top]

Emergency Services Sector

28. *May 19, Associated Press* — **Baltimore−Washington International Airport to host medical disaster drill.** One of the runways at Baltimore−Washington International Thurgood Marshall Airport in Maryland will be shut down Saturday, May 20, as military and civilian medical teams practice how to respond to a disaster that could overwhelm medical services elsewhere. A C−130 cargo plane will ferry 20 Civil Air Patrol cadets, made−up to look like military personnel wounded in an overseas bombing, from nearby Martin State Airport to BWI. Once there, they will be met by military and civilian triage teams and eventually be transported by fire and rescue companies from around the state to four hospitals. The premise of the drill is that military hospitals in the area are filled to capacity and casualties must be shipped to civilian hospitals. The Maryland Institute for Emergency Medical Services System, which licenses paramedics and other first responders and oversees the state's emergency medical system, is among the organizations participating in the drill. This test of the system is the first in Maryland in 20 years and will help identify problems such as those that occurred in the Gulf States following Hurricane Katrina.
Source: http://www.thewbalchannel.com/news/9244544/detail.html

[Return to top]

Information Technology and Telecommunications Sector

29. *May 19, eWeek* — **Alert raised for Microsoft Word zero−day attack.** A zero−day flaw in the ubiquitous Microsoft Word software program is being used in an active exploit by sophisticated hackers in China and Taiwan, according to warnings from anti−virus researchers. Symantec's DeepSight Threat Analyst Team has escalated its ThreatCon level after confirming the unpatched vulnerability is being used "against select targets." The exploit arrives as an ordinary Microsoft Word document attachment to an e−mail. However, when the document is launched by the user the vulnerability is triggered to drop a backdoor with rootkit features to mask itself from anti−virus scanners. The SANS Internet Storm Center said that it received reports of the exploit from an unnamed organization that was targeted. When the .doc attachment is opened, it exploits a previously unknown vulnerability in Microsoft Word and infects a fully patched Windows system. The exploit functioned as a dropper, extracting and launching a Trojan that immediately overwrites the original Word document with a "clean," uninfected copy. Microsoft has been notified and is working with security researchers to investigate the bug.
Source: http://www.eweek.com/article2/0,1895,1965042,00.asp

30. *May 19, Secunia* — **Microsoft Word unspecified code execution vulnerability.** A vulnerability has been reported in Microsoft Word, which can be exploited to compromise a user's system. The vulnerability is caused due to an unspecified error. This can be exploited to execute arbitrary code. NOTE: This vulnerability is being actively exploited. The vulnerability has been reported in Microsoft Word 2002 and Microsoft Word 2003.
For a complete list of vulnerable products, see source advisory.
Solution: Do not open untrusted Office documents.
Source: http://secunia.com/advisories/20153/

31. *May 19, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−139A: Microsoft Word Vulnerability.** A buffer overflow vulnerability in Microsoft Word could allow an attacker to execute arbitrary code on a vulnerable system. Systems affected: Microsoft Word 2003; Microsoft Word XP (2002). Microsoft Word is included in Microsoft Works Suite and Microsoft Office. Other versions of Word, and other Office programs may be affected or act as attack vectors. Opening a specially crafted Word document, including documents hosted on Websites or attached to e−mail messages, could trigger the vulnerability. Office documents can contain embedded objects. For example, a malicious Word document could be embedded in an Excel or PowerPoint document. Office documents other than Word documents could be used as attack vectors. For more information, please see Vulnerability Note:
VU#446012: http://www.kb.cert.org/vuls/id/446012
Solution: At the time of writing, there is no complete solution available. Consider the following workarounds: Do not open unfamiliar or unexpected Word or other Office documents, including those received as email attachments or hosted on a Website. Please see Cyber Security Tip ST04−010 for more information:
http://www.us−cert.gov/cas/tips/ST04−010.html
Also, do not rely on file extension filtering. In most cases, Windows will call Word to open a document even if the document has an unknown file extension. For example, if document.d0c (note the digit "0") contains the correct file header information, Windows will open

document.d0c with Word.
Source: http://www.uscert.gov/cas/techalerts/TA06−139A.html

32. *May 19, Secunia* — **Sun ONE/Java System Web Server cross−site scripting vulnerability.**
A vulnerability has been reported in Sun ONE and Sun Java System Web Server, which can be exploited to conduct cross−site scripting attacks. Input containing a " (double quote) character in the URL is not properly sanitized before being returned to users in error pages. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.
For a list of vulnerable products, please see source advisory.
Solution: Apply Service Pack or updates.
For Sun ONE Web Server 6.0, apply Service Pack 10 or later:
http://www.sun.com/download/products.xml?id=43a84f89
For Sun Java System Web Server 6.1, apply Service Pack 5 or later:
http://www.sun.com/download/products.xml?id=434aec1d
International version at http://www.sun.com/download/products.xml?id=43c43041
For Sun ONE Application Server 7 Platform Edition, apply Update 7 or later:
http://www.sun.com/download/products.xml?id=42ae3178
For Sun ONE Application Server 7 Standard Edition, apply Update 7 or later:
http://www.sun.com/download/products.xml?id=42ae317c
For Sun Java System Application Server 7 2004Q2 Standard Edition, apply Update 3 or later:
http://www.sun.com/download/products.xml?id=427fe06d
For Sun Java System Application Server 7 2004Q2 Enterprise Edition, apply Update 3 or later.
http://javashoplm.sun.com/ECom/d...tailId=SJAS72004Q2U3−EE−O TH−G−ES
Source: http://secunia.com/advisories/20147/

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 increased activity attempting to exploit a vulnerability in Microsoft Word.

For more information, please see
http://www.us−cert.gov/current/current_activity.html#mdroppe r

US−CERT has published the following Security Alerts:

1. Technical Cyber Security Alert: Microsoft Word Vulnerability
http://www.us−cert.gov/cas/techalerts/TA06−139A.html

2. Cyber Security Alert: Microsoft Word Vulnerability
http://www.us−cert.gov/cas/alerts/SA06−139A.html

US−CERT reports that Apple has released Apple QuickTime 7.1 to correct several vulnerabilities. Apple QuickTime 7.1 resolves multiple vulnerabilities in the way different types of image and media files are handled. An error in the AppKit framework allows an application to read characters entered into secure text field in the same window session. An attacker could exploit these vulnerabilities by convincing a user to access a specially crafted image or media file with a vulnerable version of QuickTime. Since QuickTime configures most web browsers to handle QuickTime media files, an attacker could exploit these vulnerabilities using a web page.

US−CERT recommends that Apple QuickTime users:

Upgrade their software to Apple QuickTime 7.1:
http://www.apple.com/support/downloads/quicktime71.html

Disable QuickTime in your web browser to prevent attackers from exploiting this vulnerability by persuading a user to access a specially crafted file with a web browser.

Note: Disabling QuickTime in your web browser will defend against this attack vector.

For more information please review:

Securing Your Web Browser document:
http://www.us−cert.gov/reading_room/securing_browser/

Standalone Apple QuickTime Player:
http://www.apple.com/quicktime/download/standalone.html

Mac OS X: Updating your software:
http://docs.info.apple.com/article.html?artnum=106704

VU#570689 Apple QuickTime FlashPix integer overflow:
http://www.kb.cert.org/vuls/id/570689

VU#289705 Apple Quicktime JPEG integer overflow:
http://www.kb.cert.org/vuls/id/289705

We will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 38566 (−−−), 25 (smtp), 41170 (−−−), 445 (microsoft−ds), 53 (domain), 4658 (−−−), 135 (epmap), 80 (www) 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