Department of Homeland Security Daily Open Source Infrastructure Report
for 17 August 2007

Daily Highlights

- The El Paso Times reports an FBI terrorism task force has arrested a 47−year−old Clint, Texas, man accused of shining a green laser on airplanes flying up to 35,000 feet over El Paso. (See item 9)

- The New York Police Department in a study released on Wednesday, August 15, concluded understanding how seemingly ordinary people become radicalized and hatch homegrown terror plots is essential for law enforcement officials in the United States. (See item 21)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

---

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) – http://www.esisac.com]

1. *August 16, New York Times* — **Facing the multiple risks of newer, deeper mines.** As hope dims for the six miners trapped by a coal mine collapse in central Utah, engineers and seismologists are grappling with the broader implications of the Crandall Canyon Mine accident and the interplay of risks they say are mounting in the newer, deeper generation of coal mines, especially in the West. The extreme depth of the mine, the history of mining−induced seismic activity in Utah's coal−mining region, and the method of coal recovery −− called retreat mining −− that had been done in the past all compounded the difficulties and dangers the miners faced, the experts said. Whether and how any of those factors combined to set off the

huge structural failure inside the mine on the morning of August 6, a movement of earth so intense that it measured 3.9 in magnitude and was first thought to be an earthquake, is unknown. Officials at the federal Mine Safety and Health Administration said they would not formally begin their investigation until the rescue or recovery efforts were completed. But there is little doubt, mine experts said, that retreat mining at extreme depth in Utah, where mine−produced tremors are common, creates a tapestry of forces that adds to mining's inherent hazards.
Source: http://www.nytimes.com/2007/08/16/us/16mine.html

2. *August 16, Associated Press* — **Ohio: Renewable energy plan approved.** State utility regulators approved a proposal Wednesday, August 15, by FirstEnergy Corp. to give its Ohio customers the option of purchasing energy from renewable resources. Customers can choose to purchase a monthly minimum of 200 kilowatt−hours of credits from renewable resources such as wind and solar, the Public Utilities Commission of Ohio (PUCO) said in a statement. Duke Energy Corp. already has a green pricing program running in Ohio, and American Electric Power will have its program operational in September, said PUCO spokesperson Shana Eiselstein. Akron−based FirstEnergy, the nation's fifth largest investor−owned electric system, controls seven electric utility operating companies. It serves 4.5 million customers in Ohio, Pennsylvania, and New Jersey.
Source: http://biz.yahoo.com/ap/070815/oh_renewable_energy.html?.v=1

3. *August 16, Platts Energy Bulletin* — **Twenty−six companies offer to build oil refineries in Nigeria.** Twenty−six companies have applied for licenses to build oil refineries in Nigeria, as Africa's top oil producer aims to curb imports of petroleum products, the Department of Petroleum Resources (DPR) said in a report released Thursday, August 16. The DPR, Nigeria's oil industry monitor, had earlier this year cancelled 17 of the 18 licenses it granted to investors in 2002 to build refineries in the country, after the beneficiaries failed to utilize the permits. The newly appointed Minister of State for Petroleum, Odein Ajumogobia, Tuesday said his ministry would focus on raising local supply of petroleum products. Nigeria, the world's eighth largest oil exporter, currently imports 100 percent of its fuel needs following the collapse of its four refineries. The DPR revealed in the report that only the Port Harcourt refinery was operating since 2006, at an average utilization rate of 37.92 percent of its 210,000 b/d capacity.
Source: http://www.platts.com/Oil/News/8209675.xml?sub=Oil&p=Oil/New s

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *August 15, Chicago Tribune* — **Ammonia leak spurs evacuations.** Firefighters had to evacuate two apartment buildings late Tuesday, August 14, after an ammonia leak at a frozen foods company sparked a hazardous materials response in Chicago's commercial Fulton Market area. The scene was secured just before midnight, about an hour after 12 people were evacuated from two three−story buildings in the 200 block of North Racine Avenue, said Chicago Fire Department spokesperson Eve Rodriguez. Firefighters also had set up a decontamination area at the intersection of Lake and Elizabeth Streets. The leak appeared to be coming from a pressurized line inside the business, possibly in a refrigeration system. Firefighters remained on site early Wednesday morning to continue airing out the structures.

Source: http://www.chicagotribune.com/news/local/chi−070814haz−matau g14,1,4448398.story?track=rss

5. *August 15, Associated Press* — **Gas leak closes port facility.** Port facilities at North Charleston, South Carolina were closed Wednesday, August 15, when a gas leak was discovered in a shipment bound for Europe, officials said. No injuries were reported but officials were concerned because the gas is flammable. The leak was discovered in a shipment of six cylinders containing difluoroethylene, typically used as a refrigerant, State Ports Authority spokesperson Byron Miller. The cylinder's manufacturer had crews on the way to try to stop the leak and firefighters were at the port with state and federal officials. The port was shut down at 6:30 a.m. EDT Wednesday. The chemical was to be used in a manufacturing process to coat wires used in high−temperature environments.
Source: http://www.islandpacket.com/news/state/regional/story/662269 5p−5899641c.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *August 16, Finextra (UK)* — **Fidelity hit with lawsuit over Certegy customer data theft.** A class action lawsuit has been filed against Fidelity National Information Services following the theft of 8.5 million customer records at its Certegy unit by a former database administrator who sold the information to data brokers that in turn sold it on to direct marketers. Fidelity said in July that a former employee at its Certegy unit stole 2.3 million customer records. However, according to a July 25 Securities and Exchange Commission filing, Fidelity said an on−going investigation into the incident found that approximately 8.5 million consumer records were stolen −− over three times the original estimate. Around 5.7 million of the records included checking account records, while approximately 1.5 million included confidential credit card information.
Source: http://www.finextra.com/fullstory.asp?id=17328

7. *August 16, Websense Security Labs* — **Phishing alert: AXIS Bank.** Websense Security Labs has received reports of a phishing attack that targets customers of AXIS Bank. Users receive a spoofed e−mail message asking them to renew certain services, and claiming that failure to do so will result in the suspension or deletion of the account. The e−mail provides a link to a phishing site, which attempts to collect personal and account information. This phishing site is hosted in Malaysia and was down at the time of this alert.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=793

8. *August 15, Register (UK)* — **FTC: Web scam artists pilfered $24.7m from American businesses.** After allegedly pilfering more than $24.7m from small businesses and non−profits across the country, a group of Web scam artists will fork over $1.2m to settle a court case

brought by the federal government. For several months starting in 2002, according to a suit from the Federal Trade Commission (FTC), the case's 11 defendants forced unauthorized Web charges onto hundreds of thousands of American companies, nabbing nearly $25m. Five years on, the FTC has announced that 10 of the 11 have agreed to settle, each promising not to pull the same trick again. The lone hold−out, Steven L. Kennedy, looks set for a December trial. Filed in June of 2006, the FTC suit claims that the 11 made countless cold calls to small businesses and non−profits, offering a free 15−day trial of a Website design service. But it looks like the free trial was less than free. Though operators insisted that the service would automatically cancel after 15−days if it wasn't approved by the customer, the FTC says, the defendants pushed charges onto customer phone bills whether they had approval or not.
Source: http://www.theregister.co.uk/2007/08/15/ftc_settles_with_web_scam_artists/

[Return to top]

Transportation and Border Security Sector

9. *August 16, El Paso Times* — **Laser targets planes over El Paso; Clint man held.** An FBI terrorism task force has arrested a 47−year−old Clint, TX, man accused of shining a green laser on airplanes flying up to 35,000 feet over El Paso. Clinton Udet Pinckert was arrested Tuesday night, August 14, at his home by members of the FBI Joint Terrorism Task Force after a report that a laser was shined on a commercial airplane earlier that night, officials said Wednesday. Pinckert was charged with attempting to disable commercial aircraft. If convicted, he faces up to 20 years in prison, said Daryl Fields, spokesperson for the U.S. attorney's office. He was being held at the El Paso County Jail without bond. Pinckert is accused of using a powerful Class IIIb laser, which is the size of a flashlight and used for light shows, that could potentially blind or disorient pilots, said Special Agent Andrea Simmons, spokesperson for the FBI in El Paso. In the past two weeks, at least four aircraft −− including airliners −− reported a green laser coming from Clint. Lasers pointed at aircraft has been an international concern for fears the tactic could be used by terrorists to cause a crash.
Source: http://www.elpasotimes.com/news/ci_6634262

10. *August 16, Daily News Transcript (MA)* — **Suspicious men reported seen near airport.** Two unidentified men were reportedly seen taking photos of the facilities at Norwood Memorial Airport in Norwood, MA, during the past week, prompting security concerns among police and airport officials. A woman reported the suspicious activity to police Tuesday, August 14, claiming to have seen ''two dark−skinned males walking south on Access Road near airport property'' about 7:30 EDT the previous night, according to police records. The woman further stated that she believed the two men were the same people a friend of hers saw last week taking pictures of the airport's main building, police said. A police report indicates that airport officials knew the two men were seen in the area, but not that they were seen taking pictures.
Source: http://www.dailynewstranscript.com/homepage/x2110143022

11. *August 16, NorthJersey.com* — **Fire briefly closes Teterboro Airport.** A small Gulf Stream jet briefly caught fire at Teterboro Airport Thursday, August 16, as the pilot and mechanic were testing it, a Port Authority spokesperson said. Port Authority police quickly extinguished the fire and no one was hurt, said Marc Lavorgna, a spokesperson. The airport was shut down for 10 minutes because of the incident. The plane was being fixed because it was having problems

with take−offs and landings, Lavorgna said. The plane was taxiing away from the airport's runways when the fire occurred.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnF lZUVFeXk0NSZmZ2JlbDdmN3ZxZWVFRXl5NzE4MjYyMSZ5cmlyeTdmNzE3Zjd 2cWVlRUV5eTM=

12. *August 16, Journal News (NY)* — **New program to let some fliers zip through Westchester airport security lines.** New York's Westchester County Airport on Monday, August 20, will launch a program that allows registered users to speed through the lines and get to their flights with less hassle. It's essentially like an E−ZPass for fliers. The Registered Traveler program requires users to carry an identification card with fingerprint and iris scan images and allows them to go through their own security line. Travelers can begin the application process online at or they can go to the kiosk at the airport, which will be open until the end of the month. Once biographical information is provided, applicants must scan their fingerprints and iris images. Two forms of identification, such as a passport and a driver's license, must also be scanned. This information is then submitted to the Transportation Security Administration for approval. The program is open only to United States citizens or permanent legal residents. Approved members can expect to receive their cards in two to four weeks. An annual fee of $99.95 is charged once the traveler is approved. The program will operate at no cost to the county.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/200 70816/NEWS02/708160421/1029/NEWS13

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *August 15, International Herald Tribune* — **Unidentified virus decimates China's pig population.** A highly infectious swine virus is sweeping China's pig population spawning fears of a global pandemic among domesticated pigs. So far, the mysterious virus, believed to be an unusually deadly form of an infection known as blue−ear pig disease, has spread to 25 of this country's 33 provinces and regions. The government in Beijing acknowledged that in the past year, the virus had decimated pig stocks in southern and coastal areas. But animal virus experts said that the Chinese authorities were playing down the gravity and spread of the outbreak, and had refused to cooperate with international scientists. "They haven't really explained what this virus is," said Federico Zuckermann, a professor of immunology at the College of Veterinary Medicine of the University of Illinois. "They haven't sent samples to any international body." Experts said the virus was rapidly moving from the coasts to inland and the west, to areas like this one in Sichuan Province, China's largest pork producing region. The government said that about 165,000 pigs had contracted the virus this year. Few believe the figures, particularly when pork prices have skyrocketed by more than 85 percent in the past year and field experts are reporting widespread disease outbreaks.

Source: http://www.iht.com/articles/2007/08/15/business/pigs.php

14. *August 14, Brownfield Ag News* — **More soybean rust found in southeast.** The U.S. Department of Agriculture is confirming three new cases of Asian soybean rust on soybeans in the southeastern U.S. The first case is on a private research farm in Brooks, GA, close to the Florida border. This is the first rust on beans and the fifth finding overall in Georgia. The second was in a sentinel plot in Washington, MS, in a field scheduled to be harvested this week. The plot is adjacent to another field found to have rust earlier this year. This is the furthest north rust has been found in Mississippi this year, the second with rust on beans and the third overall. The third was in St. Landry, LA. This is the thirteenth parish reporting rust and the fourteenth total thus far this year.
Source: http://www.brownfieldnetwork.com/gestalt/go.cfm?objectid=65F FE222–B479–D3C4–5A72A5FD9B7B7CF3

[Return to top]

Food Sector

15. *August 16, New York Times* — **China plans greater scrutiny of food exports.** Chinese government authorities are prepared to require that every shipment of food being exported to the U.S. and other countries be inspected for quality by the government, starting September 1, a senior Chinese trade official said on Wednesday, August 15. Zhao Baoqing, who is based at the Chinese Embassy in Washington, said that all types of food would be inspected with at least one box in each shipment checked and that each package or shipment would be affixed with a government seal. Previous vows to step up inspections in China have been met with skepticism, because many exporters of food have a tradition of mislabeling goods and shipping them illegally. The country's food safety enforcement program has historically been weak, and even prone to corruption and bribery. The enhanced food inspections, Zhao said, would not mean that every box of food would be inspected by a government official. Instead, every shipment will be checked at some point along the production line, and a higher percent of the food in individual shipments will be physically checked, he said.
Source: http://www.nytimes.com/2007/08/16/business/16inspect.html?_r =1&oref=slogin

16. *August 15, Seattle Times* — **Detainees ill.** About 300 immigrants being held at the Northwest Detention Center in Tacoma, WA, spent the early part of this week recovering from suspected food poisoning. Tacoma–Pierce County Health Department officials said they were contacted Saturday, August 11, after about 180 detainees were treated for diarrhea, nausea and vomiting at the detention–center clinic. Most began showing symptoms late Saturday, Department of Homeland Security spokesperson Lorie Dankers said, adding that detention–center staff, who sometimes eat there, also got ill.
Source: http://seattletimes.nwsource.com/html/localnews/2003836764_s ickness15m.html

[Return to top]

Water Sector

Nothing to report.

Public Health Sector

17. *August 16, Associated Press* — **Bird flu kills Indonesian teenager.** A 17−year−old Indonesian girl died of bird flu, raising the country's death toll to 83, the Health Ministry said Thursday, August 16. The girl from Tangerang, just west of capital Jakarta, died on Tuesday, August 14, after only one day after being admitted to a hospital, said spokesperson Joko Suyono. At least 193 people −− the majority of them in Indonesia −− have died worldwide from bird flu since it first infected Asian ducks and chickens in 2003, according to the World Health Organization.
Source: http://www.iht.com/articles/ap/2007/08/16/asia/AS−GEN−Indone sia−Bird−Flu.php

18. *August 16, Reuters* — **Indian flooding sparks new worries about polio.** India will make "extraordinary efforts" to immunize children against polio in its eastern state of Bihar, fearing disruption by massive flooding may make them more vulnerable to the crippling disease, officials said on Thursday, August 16. The country of 1.1 billion people has the world's highest number of polio cases, with 139 being reported in 2007 out of a global total of 345. Defeating the paralyzing disease in India is seen as key in the global war against the virus. In Bihar, where 20 cases of the virulent Type 1 polio were reported this year, nearly 15 million people −− including millions of children −− have been affected in what officials say are the worst monsoon floods in memory in some areas. The World Health Organization said with thousands of marooned or homeless children living in crowded makeshift camps in the state of 90 million people the transmission of the virus could become easier.
Source: http://www.reuters.com/article/healthNews/idUSDEL26307920070 816

19. *August 16, Agence France−Presse* — **Extortion bid halts medicine supply to Indian state.** Medicine shipments to a revolt−hit state in India's northeast have dried up after pharmaceutical firms were told to pay 250,000 dollars in extortion money, officials said on Thursday, August 16. Separatist rebels in Manipur ordered all pharmaceutical companies operating in the state to pay militants a total of 10 million rupees (250,000 dollars). The extortion demand was telephoned in to local newspapers in Manipur in early August and appeared as news reports. The state's top health official said the government was taking the demand seriously and was working with drug companies to encourage them to resume supplying Manipur. Among the thousands affected as drugs became scarce were many people living with AIDS in a region where HIV−infection rates are high. Pharmacy stores reported they were running low on many drugs and basic materials like syringes and bandages.
Source: http://news.yahoo.com/s/afp/20070816/hl_afp/indiaunresthealt haids_070816161027;_ylt=Aj47dvllr3tfk4oI5IkuQJGJOrgF

20. *August 15, W. P. Carey School of Business* — **Disease outbreak and bioterrorism: The ultimate supply chain test.** Ajay Vinze and Raghu Santanam, information systems professors at the W.P. Carey School of Business, wondered what might be the best way to allocate critical resources during a disease outbreak. They realized that, viewed from a business perspective, the public health system is actually a very large and complex supply chain. Researchers obtained a grant from the U.S. Centers for Disease Control (CDC) to study how state and local public health organizations could better address a national mandate to prepare for biological terrorism.

The two created a working computer model to determine how municipalities should best prepare for and respond to public health crises. Running the simulations for the Maricopa, AZ, Department of Public Health netted results that Santanam says are not necessarily intuitive. For example, in addressing bioterrorism and epidemics, the CDC has decided to stockpile antiviral medication in a central location rather than disperse it to states in advance of a threat. But the simulations show that in many cases, the idea of a central stockpile is not as efficient in saving lives once the disease spreads. By dispersing resources before they are needed, Vinze and Santanam found that localities could get resources faster by pooling among themselves.
Source: http://knowledge.wpcarey.asu.edu/index.cfm?fa=viewfeature&id =1456

[Return to top]

Government Sector

21. *August 16, New York Times* — **New York City police report explores homegrown terrorism.** Understanding how seemingly ordinary people become radicalized and hatch homegrown terror plots is essential for law enforcement officials in the United States and abroad to stay one step ahead, a study released on Wednesday, August 15, by the New York Police Department concluded. The study found that unassimilated Muslims in the United States are vulnerable to extremism, but less so than their European counterparts. Police analysts studied 11 cases from the past six years to better understand terrorist patterns. Their 90–page report highlighted how ordinary people in Western nations, with unremarkable jobs and with little or no criminal histories, sometimes come to adopt a terrorist ideology. It found a similar dynamic at work in recent terror plots in Britain, Spain, Canada, Australia, and the Netherlands.
Radicalization in the West and the Homegrown Threat:
http://www.nyc.gov/html/nypd/pdf/dcpi/NYPD_Report–Radicaliza tion_in_the_West.pdf
Source: http://www.nytimes.com/2007/08/16/nyregion/16terror.html

[Return to top]

Emergency Services Sector

22. *August 15, GovExec* — **IG urges better post–disaster data sharing.** The Department of Homeland Security inspector general (IG) is urging the Federal Emergency Management Agency (FEMA) to streamline information sharing to help law enforcement agencies locate missing children, registered sex offenders, and fugitive felons during disasters. A report released by the IG this week showed that after Hurricane Katrina, law enforcement agencies struggled to get information from FEMA that would have helped them track down missing children and criminals. Among those missing after the storm were 5,000 children, more than 2,000 sex offenders, and a number of fugitive felons. The FBI, New Orleans district attorney's office, and state and local law enforcement agencies had to go through a time–consuming process to gain access to FEMA's disaster recovery assistance files. The agencies were not granted direct access due to FEMA's concerns about improperly disclosing information protected by the 1974 Privacy Act. According to the report, FEMA took five to 12 days on average to fulfill law enforcement requests for information. Some requests took as many as 35 days.

Report: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07–60_Jul07.pdf
Source: http://www.govexec.com/story_page.cfm?articleid=37768&dcn=to daysnews

23. *August 15, Inside Bay Area (CA)* — **California's East Bay close to emergency radio deal.** Preparing for the next disaster in California, dozens of East Bay public agencies are close to a deal that would allow the region's firefighters and law enforcement to speak on the same radio channels during emergencies. Today these agencies in Alameda and Contra Costa counties have limited ability to talk to one another and at times must rely on their dispatchers to relay messages to first responders in the field. "There's a significant delay when you do that", said Contra Costa Fire Chief Keith Richter. "We don't want to have to do relays when the Big One hits." East Bay fire departments, law enforcement agencies and other public officials plan to hold a press conference on September 11 to announce the creation of a joint powers authority that will oversee the $100 million radio project, which could be rolled out as early as fall 2008. The system is not limited to firefighters and law enforcement. Public works crews, building inspectors and the California Department of Transportation might be needed in disasters too. Nearly every East Bay city has agreed to participate in the project, as have regional agencies.
Source: http://www.insidebayarea.com/ci_6627615?source=most_emailed

[Return to top]

Information Technology and Telecommunications Sector

24. *August 16, Associated Press* — **Many Skype users unable to make calls.** Skype, the popular computer program that lets its users make long–distance phone calls over the Internet, said Thursday, August 16, that software problems have left many of its millions of users without service worldwide. The company, a division of online auction company eBay Inc., said on its Website that many users cannot log on to the free service. It was not immediately clear how many users were affected, but Skype users in Colombia, Brazil, Germany, Finland and the United States reported difficulties logging on.
Source: http://news.yahoo.com/s/ap/20070816/ap_on_hi_te/germany_skyp e_outage;_ylt=Ah7bLjwHChRDFIVivIKlol0jtBAF

25. *August 16, CNET News* — **Adobe: No threat from PDF spam.** PDF spam —– junk e–mail with its message attached as a PDF file to get past spam filters —– poses no security risk, says Adobe Systems. Asked if PDF spam can embed malicious software, Erick Lee, a security engineer at Adobe, wrote in an e–mail on Wednesday, August 15, that "PDF is no more able to embed malware on an unsuspecting user's system than any other typical e–mail attachment." Over the last two months, security vendors have seen a spike in spam embedded within PDF documents. According to the PDF–creation software maker, there is no hard evidence that such spam exposes users to any security risk.
Source: http://news.com.com/Adobe+No+threat+from+PDF+spam/2100–7349_ 3–6202909.html?tag=nefd.top

26. *August 16, InformationWeek* — **Ubuntu tackling breach that hit half its servers.** The open–source Ubuntu project is on the mend after shutting down more than half of its servers this past weekend because they had been compromised and were launching attacks. James

Troup, who leads the Canonical sysadmin team, said in an online advisory that one of the hosted community servers that Canonical sponsored had been breached. Once technicians discovered that compromise, he said an investigation found that five of the eight machines had been breached and were actively attacking other machines. According to a notice in the Ubuntu newsletter, the servers were suffering from a few problems, such as missing security patches, FTP was being used to access the machines, and no upgrades "past breezy" were made due to problems with the network cards and kernels. Troup noted that since FTP was being used to access the machines, an attacker could have gotten access to the servers by sniffing the clear−text passwords.
Source: http://www.informationweek.com/software/showArticle.jhtml;js essionid=2GV0M1R5OEZCCQSNDLOSKHSCJUNN2JVN?articleID=20180054 5

27. *August 15, IDG News Service* — **New URI browser flaws worse than first thought.** Security researchers Billy Rios and Nathan McFeters say they've discovered a new way that the URI (Uniform Resource Identifier) protocol handler technology, used by Windows to launch programs through the browser, can be misused to steal data from a victim's computer. URI bugs have become a hot topic over the past month ever since researcher Thor Larholm showed how a browser could be tricked into sending malformed data to Firefox using this technology. Later, other researchers, including Rios and McFetters, showed how other browsers and applications could be misused to achieve similar goals. In the past days, however, Rios and McFetters have shifted their focus away from malformed data and have taken a close look at how attackers could simply misuse the legitimate features of software that is launched via the URI protocol handler, something they call "functionality based exploitation." Their initial results show that there could be plenty of ways to misuse this technology. Rios and McFetters plan to release the results of their research after the vendor has had a chance to fix the problem.
Source: http://www.infoworld.com/article/07/08/15/New−URI−browser−fl aws−worse−than−first−thought_1.html

28. *August 15, ComputerWorld* — **Fake plain−text e−card variants look real, carry computer viruses.** A new form of fake e−card notification e−mails are unleashing nasty viruses and virus−carrying Trojan horses on unsuspecting users. While e−card−triggered viruses and Trojan horses are not new, the latest versions are becoming more difficult for typical antivirus and antispam defenses to detect, according to alerts issued Wednesday, August 15, by security software vendors Avinti Inc. and F−Secure Corp. The new complication, said Dave Green, chief technology officer at Avinti, is that the latest slew of fake e−card e−mail notifications are using plain text in their messages, which don't get scanned and scrutinized by antivirus and antispam defense applications. While the e−mails don't contain pasted links or attached files that a recipient can click on to get a computer infection, many e−mail clients automatically convert the included text into a clickable link when the e−mail clients recognize a Web address in the text. All recipients have to do to trigger the virus is to click on the link created by the e−mail client once they have read the message, he said. The damaging payload files are new variants of the Storm Worm virus that was first detected in January, the company said.
Source: http://www.computerworld.com/action/article.do?command=viewA rticleBasic&articleId=9030860&pageNumber=1

Internet Alert Dashboard

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

29. *August 16, CNN* — **Jury finds Padilla guilty on terror charges.** The jury in the Jose Padilla terror trial has found the American guilty of conspiracy to support Islamic terrorism overseas. Padilla was originally arrested on accusations that he planned to set off radioactive "dirty bombs" in the United States. Thursday, August 16's convictions are not related to those accusations, and prosecutors did not present the "dirty bomb" plot to the jury. Padilla's two co−defendants, Adham Hassoun and Kifan Jayyousi, were also found guilty on the three counts as charged: conspiracy to murder, kidnap, and maim people in a foreign country; conspiracy to provide material support for terrorists; and providing material support for terrorists. The verdict came after less than two days of deliberations by the federal jury in Miami. Sentencing is set for December 5. All three defendants face life in prison.
Source: http://www.cnn.com/2007/US/08/16/padilla.verdict/?iref=mpsto ryview

[Return to top]

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.