Department of Homeland Security Daily Open Source Infrastructure Report for 13 February 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- The New York Times reports an audit by the Government Accountability Office shows that the U.S. Nuclear Regulatory Commission has underestimated the risk of a terrorist attack on a nuclear research reactor on a college campus and the potential consequences of such an attack. The NRC's executive director says the GAO audit "lacks a sound technical basis." (See item **8**)
- According to the Washington Post, the European Commission will propose on Wednesday that all foreign travelers entering and exiting Europe, including American citizens, should be fingerprinted. If approved by the European Parliament, the proposal would mean that information on tens of millions of citizens will be added in coming years to databases that could be shared by friendly governments worldwide. (See item **14**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

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

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

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. *February 12, News-Leader* – (Missouri) **CU anticipates outages, calls for crews to help.** City Utilities (CU) has summoned help from three Missouri cities in anticipation of additional power outages today, according to a CU spokesman. The Springfield-based utility went to emergency status Monday afternoon – automatically putting crews on 16-hour work days. A short time later, it asked for 23 line crews and ten tree-trimming

crews from Kansas City, Joplin, and Clinton. “We’re watching that system out of Tulsa very closely,” the spokesman said. “By no means are we out of the woods with this yet.” About 5,000 power outages were reported Monday evening. Those outages began in the southwest part of CU’s system, the spokesman said. Most were caused by downed tree limbs and ice-laden “hangers” falling out of trees. Any CU customer who loses power should call the utility to report it. However, if a downed power line is arcing or sparking or poses an imminent threat to safety, the spokesman urged people to call 911.
Source: http://www.news-leader.com/apps/pbcs.dll/article?AID=/20080212/NEWS01/802120351

2. *February 12, Lexington Herald-Leader* – (Kentucky) **Marathon oil line spills at Clark farm.** A 24-inch oil line ruptured Monday in a rural area of Clark County, Kentucky, officials said. The spill was discovered about 9:15 a.m. Some of the oil spilled into a farm pond. About 200 barrels, or 8,400 gallons, had spilled as of 1:15 p.m., said a manager for Kentucky Emergency Management (KEM). The pipeline runs to the Marathon oil refinery in Eastern Kentucky. The spill is contained in the pond, said a spokeswoman for Marathon. Cleanup will probably continue for the next couple of days. Officials continue to investigate where the spill took place and what caused it. The manager for KEM said the spill was not a threat to the water supply. Personnel from the State Division of Emergency Management and Department of Environmental Protection responded to the spill.
Source: http://www.kentucky.com/211/story/315631.html

3. *February 10, San Diego Union-Tribune* – (California) **Power-line tie-downs a fire hazard?** Power lines are known to be a fire danger, especially in rural areas thick with brush and susceptible to high winds. At least three of the wildfires that ravaged San Diego County in October were started by the electric grid. Less known is that the cable systems that tie down at least ten – perhaps hundreds – of the power poles planted throughout the backcountry may also pose a threat because they are capable of conducting electricity. The hazard occurs when support cables loosen and sway in heavy winds, creating the potential for arcing – sporadic sparks that can ignite weeds and other vegetation. The power-pole design was declared dangerous by an independent analyst retained by an insurance company to examine potential causes of the October fires. There is no proven link between the design and the fires, but the consultant’s findings have prompted state utility regulators to open their own investigation. San Diego Gas & Electric Co. (SDGE) says its system is safe and complies with state regulations. Regular inspections have found no evidence of arcing in the backcountry transmission system, a utility spokeswoman said. Officials at the California Public Utilities Commission, which regulates SDGE and other investor-owned utilities, agreed that the 69,000-volt transmission system does not appear to violate regulations. But they are troubled by the design and said rule changes may be needed to address their concerns, which for now are limited to SDGE, even though other power companies may use similar systems. An expert on electrical transmission said one solution might be to apply some form of chemical or plastic sealant to the connection between the support cables and anchor rods, so they are not as susceptible to looseness during wind gusts.
Source: http://www.signonsandiego.com/news/metro/20080210-9999-1n10sdge.html

[Return to top]

Chemical Industry Sector

4. *February 12, Park Rapids Enterprise* – (Minnesota) **Park Rapids Schools plan mock drill Wednesday.** The Park Rapids Schools and local emergency responders will be conducting a mock drill at 1:45 p.m. on Wednesday at both Century School and the Area High School. The exercise will include a lock down and evacuation. All schools in Minnesota are required to do similar exercises. The drill planned for Wednesday will simulate a chemical spill or gas leak.
   Source: http://www.parkrapidsenterprise.com/articles/index.cfm?id=11030

5. *February 12, Associated Press* – (Connecticut) **Truck leaking hydrogen shuts Conn. Highway.** Dozens of homes have been evacuated because an overturned tractor trailer is leaking hydrogen gas on Interstate 84. The road's closure is causing major traffic problems in the area. The rig overturned about 5:30 a.m. Tuesday and both lanes of the major thoroughfare are closed, state police said. Hydrogen gas is highly explosive. The State Department of Transportation said the accident would take several hours to clear. The heavily-used highway is one of the main routes from Massachusetts into New York State.
   Source: http://www.msnbc.msn.com/id/23125962/

6. *February 11, WKRG 5 Pensacola* – (Alabama) **Chemical leak.** Neighbors in McIntosh, Alabama, were told to stay inside Monday morning when a chemical leak was discovered at the Ciba plant. It happened around 6:30 Monday morning. A Ciba Emergency Response manager says the chemical leaking was hydrochloric acid and that the leak has been contained. Now, a team is looking into what exactly caused it; "that process is ongoing right now to understand what is failed and of course specifically what we can do to prevent that from happening again," he said. Classes at both McIntosh elementary and high school were cancelled for the day because of the chemical leak. A plant worker who inhaled the hydrochloric acid fumes was taken to a hospital in Mobile to get checked out.
   Source: http://www.wkrg.com/news/article/chemical_leak/10174/

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

7. *February 12, Herald News* – (Illinois) **Nuclear plant leaks tritium again.** An Exelon employee recently noticed a puddle that appeared to be bubbling near a building at the Braidwood nuclear plant in Will County, Illinois. Testing revealed the puddle contained a small amount of tritium leaking from an underground pipe. The puddle "contained 878 picocuries per liter of tritium," said an Exelon Braidwood spokesman. Tritium is a radioactive hydrogen isotope that is also a byproduct of nuclear reactors producing electricity. High levels of tritium are thought to cause cancer. The U.S. Environmental Protection Agency has established an upper limit for tritium concentration in drinking water of 20,000 picocuries per liter. Exelon officials have maintained the levels released

were well below that amount. The leak happened around 10 p.m. February 5 and was discovered around 8 a.m. February 6, according to the spokesman. The leak was in a pipe that was buried about eight feet underground. The pipe was excavated and capped by 6:30 p.m. Saturday. "Our personnel are continuing to monitor it to determine if further mediation is necessary," the spokesman said. "The leak is centered on our property and posed no hazard to our employees or the public."
Source:
http://www.suburbanchicagonews.com/heraldnews/news/788487,4_1_JO12_TRITIUM_S1.article

8. *February 11, New York Times* – (National) **Threat to campus reactors cited.** The risk of a terrorist attack on a nuclear research reactor on a college campus and the potential consequences have been underestimated by the U.S. Nuclear Regulatory Commission (NRC), according to an audit by the Government Accountability Office (GAO). An unclassified version of the audit found uncertainty "about whether NRC's assessment reflects the full range of security risks and potential consequences of an attack on a research reactor." The rules, the audit said, "may need immediate strengthening," and said that more parts of research reactors are probably vulnerable to damage than the NRC assumes. Security requirements at the research reactors have changed very little since the attacks of September 11, 2001, according to the auditors, even though many of the reactors still run on enriched uranium, which terrorists could convert into fuel for an atomic bomb. In contrast, the rules for civilian power plants have become much stricter, according to the report. The NRC's executive director said in a letter of rebuttal to the GAO that the auditors did not cite any intelligence information to show that potential terrorists had the "highly sophisticated methods and skills" that the report said were within their capabilities. The audit "lacks a sound technical basis," and the GAO "failed to acknowledge key scientific facts," he wrote.
Source: http://www.nytimes.com/2008/02/11/washington/11cnd-nuke.html?_r=2&hp&oref=slogin&oref=slogin

[Return to top]

Defense Industrial Base Sector

9. *February 11, Defense News* – (National) **JLTVs to incorporate active protection systems.** The U.S. Army's next-generation Humvee, intended to incarnate an unprecedented combination of mobility and survivability, could carry defensive systems to shoot down incoming weapons. The Joint Light Tactical Vehicle (JLTV) requirements may include an active protection system (APS), which combines sensors, fire-control computer, and interceptors to provide the defenses of armor without the weight. "What all the teams are aggressively doing is looking at options other than steel plates," said Northrop Grumman's vice president of land combat. An advantage of some systems is that they can come off as demanded. "APS represents plug-and-play capability, allowing a vehicle to run around a post or station hauling the mail and be the same vehicle able to go into harm's way," he said. Whoever makes the APS that winds up on a JLTV, it will likely be lighter than the ones developed to protect the Army's 27-ton Future Combat Systems vehicles. One of these is Iron Curtain, a 300- to 500-pound

system that fires an interceptor from the roof of an up-armored Humvee at incoming RPGs, anti-tank guided missiles, and other weapons. The Defense Advanced Research Project Agency has spent about $8 million on Iron Curtain since 2005. The goal is a system that will protect two sides of a Humvee for $50,000 or less, said the president of Artis, the maker of the system.
Source: http://www.defensenews.com/story.php?F=3343210&C=navwar

10. *February 11, Washington Technology* – (National) **Raytheon to tackle satellite upgrade.** Raytheon Co. will upgrade a satellite communications system that provides protected communications to warfighters worldwide under a new Air Force contract that could be worth more than $75 million. Raytheon will develop and produce the Minuteman Minimum Essential Emergency Communications Network program, a satellite communications system of ground-based communication terminals. The Air Force expects to field the terminals for operational test and evaluation in late 2009. The solution fits with the Department of Defense's plans to have its advanced, extremely high-frequency satellite constellation in operation in 2010.
Source: http://www.washingtontechnology.com/online/1_1/32251-1.html?topic=contract-awards

[Return to top]

Banking and Finance Sector

11. *February 12, Lompoc Record* – (National) **Alert issued concerning Internet 'phishing' scam.** The Central Coast's Better Business Bureau has received at least 15 complaints regarding a new Internet "phishing" scam, officials said recently. The Better Business Bureau of the Tri-Counties has released an alert in response to the scam. Unsuspecting recipients are receiving e-mails informing them that a complaint against them or their business has been lodged with the Department of Justice, the Better Business Bureau, the Internal Revenue Service, or other regulatory organization. Designed to appear as legitimate messages from regulatory organizations, the e-mails address the recipients by name, and may contain other personal information, the FBI reported. The e-mails refer to the complaint in question, which is said to be in an attachment. However, when the recipient clicks on the attachment, instead of viewing a complaint, a virus used to steal passwords actually is downloaded. What makes things worse, the FBI said, is the virus is wrapped in a screensaver file, making it difficult for most anti-virus programs to detect the malicious intent. Once downloaded, the virus monitors user name and password logins and records the activity, as well as other password-type information entered on the compromised machine. Meanwhile, representatives of the local BBB office said they have fielded a number of calls regarding the "phishing" scam. An administrative assistant said most of the calls she has received came from area businesses, but that one government agency has also reported receiving the e-mail. Officials warn people to be wary of any e-mails received from an unknown sender. Those who received a scam should email and file a complaint at www.ic3.gov.
Source:
http://www.lompocrecord.com/articles/2008/02/12/news/centralcoast/news03.txt

12. *February 12, Chicago Tribune* – (National) **High-tech Social Security cards may join battle against ID theft.** In an effort to help combat identity theft and fraud, two Illinois congressmen are expected to introduce legislation Tuesday they hope will enhance the security features of Social Security cards. The proposed cards would feature a photograph and fingerprint, as well as a computer chip, bar code, and magnetic strip. The cards would be modeled after the Common Access Card issued by the Department of Defense, mostly to active military reserve members and their dependents, said a sponsor of the bill. Current Social Security cards have limited security features and have no photo or biometric data, he said. "One of the ways that modern criminals use to attack ... is by falsifying or counterfeiting Social Security cards," he said. "We think that a Social Security card should be hard to forge [and] that it should also make it easy to catch an identity-theft crime." A co-sponsor of the bill said that more than $49 billion a year is lost because of identity theft. According to a 2005 report by the Government Accountability Office, employers reported the use of 1.4 million Social Security numbers that do not exist.
    Source: http://www.chicagotribune.com/news/local/chi-securitycard_12feb12,0,471611.story

13. *February 11, Consumer Affairs* – (National) **Caution: Scam warning is a scam.** When a spam email went out last month, disguised as a message from Valley National Bank's security department, the bank quickly responded, posting a warning on its Web site. "A fraudulent e-mail has circulated to some Valley customers claiming that the bank has temporarily suspended their account due to "Billing Failure," the warning states. "This e-mail also provides a link to click on in order to complete an account update to unlock their account." The bank, which has 175 branches in New York and New Jersey, says the e-mails are not legitimate and should be deleted. It points out that clicking on the link will take victims to a bogus site where they will be asked to reveal username, password, and other sensitive data. But the scammers have moved on to "phase two" of their scam operation. Millions of other spam emails are now hitting inboxes, purporting to be warnings from the bank about this very scam. "Members and Non-Members may have received an e-mail that 'appears' to be from VALLEY NATIONAL BANK," the bogus email reads. "This is an e-mail fraud attempt designed by hackers to obtain your personal information. The e-mail has a link that sends you to a site similar to our Internet Branch site and requests you to supply your card information. We urge you not to follow the links or enter any account information." So, the scammer is sending out an email warning consumers about his own scam. As one reads further, the hook is revealed. "For your security, your online banking profile has been locked," the email says. "Unlocking your profile will take approximately one minute to complete." The email then gives not a Web link, but a toll-free number to call. Of course, those who call will be asked to provide their username, password, and other sensitive information. But the scammer is betting consumers will fall for it, because the scam is delivered in the form of a warning about the scam.
    Source: http://www.consumeraffairs.com/news04/2008/02/bank_scam.html

[Return to top]

Transportation Sector

14. *February 12, Fox News* – (International) **Report: Europe may begin fingerprinting foreign travelers.** The European Commission is set to propose on Wednesday that all foreign travelers entering and exiting Europe, including American citizens, should be fingerprinted, the Washington Post reported Tuesday. If approved by the European Parliament, the proposal would mean that precisely identifying information on tens of millions of citizens will be added in coming years to databases that could be shared by friendly governments around the world, the paper reported. The plan is part of a growing trend to collect and share data to identify and track people to combat illegal migration, terrorism, and organized crime.
Source: http://www.foxnews.com/story/0,2933,330391,00.html

15. *February 11, Associated Press* – (National) **More screening planned at 7 airports.** To increase security and weed out potential terrorists, workers at seven airports nationwide will undergo more vigorous screening beginning in May. The additional checks are part of a 90-day test program run by the federal Transportation Security Administration (TSA). People who work at airports across the country already receive some screening – such as background checks and random searches – before they are given access to secure areas, said a TSA spokesman. Some airport workers have unfettered access to aircraft and potentially dangerous materials. Officials are concerned that people with bad intentions could pose as airport workers and gain access to these areas. The screening tests will be conducted at airports in Boston; Denver; Kansas City; Jacksonville, Florida; New Bern, North Carolina; and Eugene and North Bend, Oregon. Screening procedures will vary by airport. A total of 53,000 workers will be affected by these screening tests. Congress mandated the screening test programs late last year.
Source:
http://ap.google.com/article/ALeqM5jfdsxooK9vbfdMNjp5GRQdObBU8gD8UOCCLO0

16. *February 10, News Tribune* – (Missouri) **Man allegedly steals plane from local airport, flies it to his home.** A former employee of a business at the Jefferson City Memorial Airport, Missouri, is free on bond after allegedly stealing an airplane and flying it to Callaway County on Friday. The man is charged with one count of second-degree burglary for unlawfully entering Jefferson City Flying Service and first-degree tampering for operating a plane without the consent of the owner. According to the probable cause statement from Jefferson City police, the man used a hidden key to enter the business. He then took a key to a Cessna 150 airplane, took off from the airport, and flew to his home in Auxvasse where he landed the aircraft. The airplane became stuck in the field he had landed in, and the suspect was unable to free the aircraft. He was taken into custody shortly after.
Source:
http://www.newstribune.com/articles/2008/02/10/news_local/325local04steal.txt

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

17. *February 11, Reuters* – (National) **USDA moves to bolster food aid.** The U.S. Agriculture Department (USDA) is putting more surplus wheat on the market in order to bolster supplies at food banks and help public nutrition programs, the USDA said on Monday. The USDA, through a private vendor, will sell 1,200 bushels of soft white wheat, 889,000 bushels of durum wheat, and 3.04 million bushels of hard red spring wheat. The proceeds of the sale will be used in government nutrition programs, such as food banks, school lunch programs, or assistance to seniors, said a USDA official. The USDA has been selling government-owned commodities like corn and soybeans – which it obtains when farmers forfeit on price-support loans – for use in public nutrition programs since last summer. The barters are designed to save money on storage and bolster food assistance budgets that have been stretched by rising food costs. According the USDA, food prices are expected to rise three to four percent in 2009 as retailers pass on to consumers the costs of higher commodity and energy prices. The USDA also keeps 33.6 million bushels of wheat in reserve for international food aid donations. Source: http://www.reuters.com/article/politicsNews/idUSN1138209520080211?sp=true

[Return to top]

Water Sector

18. *February 10, WBBH 2 Fort Myers* – (Florida) **Residents concerned about contaminated water supply.** Sunday night, water experts and the Department of Health were out taking samples while trying to determine how E. coli is getting into the drinking water of Fort Myers, Florida. Boil water notices went out Friday to residents after a sample tested positive for E. coli. The notice remains in effect until further notice. Officials said that they have not found the source, are working to find the problem, and plan to have it corrected by Monday. E. coli presence in the water means the supply could be contaminated with human or animal waste. Until the notice is lifted, health officials strongly suggest that residents boil all water used for drinking, cooking, and brushing teeth.
Source: http://www.nbc-2.com/articles/readarticle.asp?articleid=17438&z=3

[Return to top]

Public Health and Healthcare Sector

19. *February 12, Chicago Tribune* – (National) **Blood-drug supply may thin.** The federal government Monday braced U.S. health facilities for potential shortages of heparin, a

popular blood thinner, after Baxter International Inc. stopped making certain heparin vials over concerns of mysterious allergic reactions in some patients receiving high dosages. The U.S. Food and Drug Administration (FDA) said potentially dangerous and "life-threatening" allergic reactions have been linked to multidose vials of heparin. Four people have died after receiving heparin, but the FDA said these cases did not "follow the pattern" of patients experiencing reactions from initial high dosages. Still, the FDA said the concerns are serious enough that hospitals should consider switching to another maker. Baxter makes 35 million vials annually, or half the U.S. hospital supply of heparin, making federal officials concerned about a growing problem, especially if the agency uncovers more adverse events with patients.
Source: http://www.chicagotribune.com/features/lifestyle/health/chi-tue_baxter2.12feb12,1,6622874.story

20. *February 11, Citizens Voice* – (Pennsylvania) **Number of flu cases increasing sharply across Pennsylvania.** Laboratory-confirmed cases of influenza across Pennsylvania have risen sharply in recent weeks, pushing the statewide total through early February to 1,940, according to state Department of Health figures. That is well ahead of the pace a year ago, when Pennsylvania experienced its mildest flu season since the department started tracking cases in 2003, with fewer than 4,000 cases reported. Only flu cases that have been confirmed through laboratory testing are reported to the state, and those represent only a fraction of state residents who have contracted the flu, a health department spokeswoman said. Typically, people do not seek medical attention for the flu and are not tested, she said.
Source: http://www.citizensvoice.com/site/news.cfm?newsid=19282560&BRD=2259&PAG=461&dept_id=455154&rfi=6

21. *February 11, Associated Press* – (Alabama) **Ala. sues AstraZeneca over drug prices.** An attorney representing the state of Alabama in a law suit against AstraZeneca said Monday that a British pharmaceutical company set up a scheme to make the Alabama Medicaid system pay $40 million too much for drugs prescribed for its patients. AstraZeneca is one of more than 70 pharmaceutical manufacturers that Alabama's Attorney General filed suit against in 2005 over drug prices. The case against AstraZeneca is the first to go to trial. The state has settled with Takeda Pharmaceuticals North America Inc. and Day LP.
Source: http://money.cnn.com/news/newsfeeds/articles/apwire/eb48383a6e313e661f4ec1973ebba109.htm

Government Facilities Sector

22. *February 11, Government Executive* – (National) **Federal Protective Service woes could threaten building security.** The Federal Protective Service's (FPS) budget shortfalls and shrinking workforce could threaten the physical security of government buildings, according to preliminary findings from the Government Accountability Office

(GAO). FPS, the agency charged with providing physical security and law enforcement services to approximately 8,800 facilities owned or leased by the General Services Administration, was transferred in 2003 from GSA to the Homeland Security Department's Immigration and Customs Enforcement bureau. Since then, FPS has faced multimillion-dollar funding shortages and ensuing management challenges. Faced with a projected revenue shortfall of $70 million for fiscal 2006, FPS restricted hiring and employee travel, limited training and overtime, and eliminated employee performance awards as belt-tightening measures. But GAO said these steps ultimately could hinder the service's ability to meet its mission.
Source: http://govexec.com/dailyfed/0208/021108e2.htm

23. *February 11, Fox News* – (District of Columbia) **Explosives found in Capitol Hill gunman's truck.** Explosives have been found in the impounded pickup truck driven by the man discovered carrying a loaded shotgun on Capitol Hill last month, U.S. Capitol police said. The truck was impounded at the Government Printing Office garage on Capitol Hill, not far from where the incident unfolded. Police executed a search warrant Friday.
Source: http://www.foxnews.com/story/0,2933,330375,00.html

24. *February 11, Register-Mail* – (Illinois) **School bomb threat under investigation.** Police are investigating a bomb threat made to Lombard Middle School Saturday night. According to reports, a male caller phoned 911 at 6:02 p.m. Saturday and said obscenities to the police dispatcher. Police believe the same caller then phoned in a bomb threat to Lombard Middle School at 6:04 p.m. Saturday. Police swept inside and outside the school, and no bomb was found. The school was evacuated as a precaution. It was unclear how many people were at the school at the time of the bomb threat.
Source: http://www.galesburg.com/news/x1973325127

[Return to top]

Emergency Services Sector

25. *February 12, Associated Press* – (National) **FEMA looks at trains for evacuations.** The Federal Emergency Management Agency (FEMA) may expand the use of passenger trains to evacuate the sick and elderly in advance of hurricanes across the Gulf Coast, a FEMA official said. A FEMA assistant administrator told a congressional subcommittee meeting in New Orleans on Monday that his agency is looking at passenger trains as a method of getting people out of harm's way. After Hurricane Katrina hit in August 2005, Amtrak was hired to be on hand to evacuate people with special needs if another disaster hit. He said FEMA is now devising disaster plans for other Gulf Coast cities based on the New Orleans model. "We're changing our whole planning focus now from Louisiana-centric to Gulf Coast-centric," he told the subcommittee. But, he said, turning railways into evacuation routes will not be easy. Rights of way for most railroads are privately owned by freight companies, and there is no congressional mandate to use railroads for evacuations. Also, the existing stock of passenger cars cannot accommodate evacuees unable to walk, he said.

Source:
http://ap.google.com/article/ALeqM5gKaW0zG_fILlBNNiq4kn6XozVPnwD8UOODGO0

[Return to top]

Information Technology

26. *February 11, InfoWorld* – (International) **Mapping out Web apps attacks.** Attackers continue to use well-worn techniques, such as SQL injection, to exploit holes in popular Web applications, but have also moved on to other targets, including government sites, and newer exploit methods, such as cross-site request forgery, according to the latest report filed by the Web Applications Security Consortium (WASC). The nonprofit industry group released the findings of its annual Hacking Incidents Database report this week. Despite the fact that cyber-criminals are still capable of using familiar means like SQL injection to victimize e-commerce sites and other transactional systems, a growing number of assailants are broadening their efforts and capabilities and going after new sets of targets, the research contends. Based on WASC's in-depth investigations into roughly 80 individual attacks carried out during the calendar year of 2007, the group concludes that data theft remains the primary goal of most incidents, representing 42 percent of all the events. Surprisingly, site defacement – thought to be a dying art in the world of profit-driven hacking – actually still accounted for 23 percent of the attacks covered in the report, followed by exploits aimed at planting malware on sites at roughly 15 percent. And while the lion's share of the incidents studied by the group revolved around the attempted theft of sensitive data that could be sold on the underground market or used to carry out fraud, the phishing threats of years past are increasingly outnumbered by attacks that utilize malware code hidden on legitimate Web applications to victimize unsuspecting end-users, the group said.
Source:
http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/08/02/11/Mapping-out-Web-apps-attacks_1.html

Internet Alert Dashboard

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]

Communications Sector

27. *February 12, Associated Press* – (National) **BlackBerry outage frustrates users again.** BlackBerry outages are rare, but when they do hit, like one did Monday that wiped out service across the U.S. and Canada, subscribers who have become addicted to the smart phones are quick to unleash their fury. It was not immediately clear late Monday what

caused the outage – the second widespread disruption in less than a year. Some users reported being able to access their service normally. Research in Motion Ltd., the Waterloo, Ontario-based company that makes the mobile device, said late Monday that customers "experienced intermittent delays" beginning around 3:30 p.m., but data service was restored about three hours later. The company said voice and text messaging services were not affected. "No messages were lost and message queues began to be cleared after normal service levels were restored," RIM said, apologizing to customers for the inconvenience. The company did not say how many customers were affected, though officials with AT&T Inc. and Verizon Wireless said RIM told them the outage hit customers of all wireless carriers. Bell Canada's spokesman said the majority of its BlackBerry customers were affected. RIM has 12 million subscribers worldwide and has deals with scores of wireless carriers to offer the BlackBerry service around the world.
Source:
http://news.yahoo.com/s/ap/20080212/ap_on_hi_te/blackberry_outage;_ylt=Ak8Lzgzjuxu T34K9UpH61vkjtBAF

28. *February 11, Associated Press* – (National) **White-space converter fizzles, again.** Technology companies eager to grab vacant airwaves and use them for high-speed Internet service first have to develop a gizmo that makes the conversion possible. Last week, a prototype device broke down again – the second time in seven months – in the hands of the Federal Communications Commission (FCC). Regulators there must be convinced that the airwaves can be used for broadband service in a way that does not interfere with other television programming and wireless microphone signals. An FCC spokesman declined to comment on the matter. The director of wireless incubation for Microsoft Corp., one of the companies developing the prototype, said the device lost power after continual testing. Technical glitches are not the only power issues facing the high-tech coalition, whose members also include Google Inc., Dell Inc., Hewlett-Packard Co., Intel Corp., EarthLink Inc., and Philips Electronics North America Corp. The coalition is in a public relations squabble with TV broadcasters, who fear such technology will interfere with their programming. The fight over so-called "white spaces" is heating up in anticipation of the February 2009 switch from analog to digital signals. Broadcasters quickly channeled the device's break down as evidence of interference risks. The FCC in late July said the coalition's first device did not reliably detect unoccupied spectrum and could interfere with other TV programming and wireless microphone signals. In that case, Microsoft said the device was simply broken and failed to work. This time, the company said the device lost power after continual testing and insists it is not a setback.
Source: http://ap.google.com/article/ALeqM5g5pA_d7JU6VvsdvIh_Kncc2j--xQD8UOD0C00

[Return to top]

Commercial Facilities Sector

29. *February 11, News-Herald* – (Ohio) **Wal-Mart evacuated in Eastlake.** A Wal-Mart in Eastlake, Ohio, was closed for approximately one hour Monday afternoon because of a phoned-in bomb threat, according to an Eastlake police official. The store was evacuated

about 3 p.m. and remained closed until 4 p.m., said a Wal-Mart spokesman. The store is working with police on the incident, and the matter is still under investigation. No other information was released.
Source: http://www.zwire.com/site/news.cfm?newsid=19284859&BRD=1698&PAG=461&dept_id=21849&rfi=6

[Return to top]

National Monuments & Icons Sector

Nothing to report.

[Return to top]

Dams Sector

30. *February 12, Augusta Chronicle* – (Georgia) **No money on way for decaying dam.** In Georgia, the New Savannah Bluff Lock & Dam was recommended for demolition in 2000 after the U.S. Army Corps of Engineers concluded it no longer served commercial navigation – the purpose for which it was built in 1937. Industries and municipalities that depend on the dam's upstream pool for drinking water and industrial uses did not want the concrete dam removed. They agreed to assume ownership of the federal project if Congress would finance the repairs. That was eight years ago, when repairs were estimated at $5.3 million. The estimate has since risen to about $22 million in 2005. A Corps spokesman – noting no repair funds were authorized in fiscal 2008 or in the fiscal 2009 civil works budget unveiled earlier this month – said the estimate will probably have to be calculated yet again. Augusta, Georgia, officials have voiced concerns in past years that if Congress never funds the repairs, the dam could become a safety hazard and the Corps might end up demolishing it anyway.
Source: http://chronicle.augusta.com/stories/021208/met_186999.shtml

31. *February 11, KOCO 5 Oklahoma City* – (Oklahoma) **Officials hope funds will remedy dam problems.** Officials with Oklahoma's conservation districts said the state's dam control system is flooded with problems and desperately needs money to fix them. "The flood control protection system that we have that protects our homes, protects our businesses, protects a lot of our farmland really was damaged by those rain events this past year," said the executive director of the Oklahoma Association of Conservation Districts. The OACD will get $30 million, half of which is to fix dams, officials said. The other half will go to fix breached farm ponds and washed-out roads, terraces, and waterways.
Source: http://www.koco.com/news/15272628/detail.html

[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 NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Distribution Information:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 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.