Homeland Security

Daily Open Source Infrastructure Report
30 November 2011

Top Stories

- A cellphone service that is supposed to grant priority to emergency government and public safety calls failed during the August earthquake that rocked the East Coast, a DHS official said November 28. – *NextGov* (See item **32**)
- Researchers found a HP LaserJet printer vulnerability that could allow hackers to remotely control the device to launch cyberattacks, steal data, and even instruct its components to overload until it catches fire. – *Softpedia* (See item **36**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *November 28, Deseret News* – (Utah) **Fiery semi crash closes U.S. 40 near Daniel's Summit.** A fiery crash November 28 involving two semitrailers closed U.S. 40 in both directions for about 4 hours between the Daniels Port of Entry and Soldier Creek Dam in Heber City, Utah. A semi hauling crude oil was traveling east on U.S. 40 about 1:30 p.m. when it was hit from behind by another semi, said a Utah Department of Public Safety spokesman. The oil tanker caught fire, but the driver was able to escape without injury. The driver of the other semi, a gas tanker with an empty load, also was

uninjured. Crews battled the fire for a few hours before it burned itself out. U.S. 40 was reopened about 5:30 p.m.
Source: http://www.deseretnews.com/article/705395027/Fiery-semi-crash-closes-US-40-near-Daniels-Summit.html

2. *November 28, Charleston Gazette* – (National) **MSHA not catching 'scofflaw violators,' report says.** Investigators from the U.S. Department of Labor's Office of Inspector General have found that federal regulators are not identifying "scofflaw violators" who do not pay mine safety and health fines, allowing those mine operators to avoid debt-collection lawsuits or other enforcement actions. The department's Mine Safety and Health Administration (MSHA) "does not have an accurate view" of the amount of delinquent fines it is owed or when the violations that drew those fines were committed, according to the Inspector General's (IG) report. The report on MSHA fines comes just 7 weeks after another IG investigation found agency officials publicly overstated their rate for completing required inspections of non-coal mines. And the IG's latest findings show continuing problems with MSHA's enforcement practices, following the agency's admission in 2008 it allowed the industry to avoid required monetary penalties for 5,000 safety violations dating back more than a decade. IG investigators examined MSHA's record collecting fines that were finalized in 2009 and 2010, and found agency officials had collected 85 percent of the $147 million in penalties.
Source: http://wvgazette.com/News/201111280229

[Return to top]

Chemical Industry Sector

3. *November 29, Louisville Courier-Journal* – (Kentucky) **American Synthetic Rubber Co. can change chemicals.** The Louisville Metro Air Pollution Control District in Louisville, Kentucky, has granted the American Synthetic Rubber Co. plant in Rubbertown a permit to phase out toluene and replace it with chemicals the district and company say are less hazardous. The firm can now start its first phase of replacing the use of toluene as an organic solvent with a mixture of cyclohexane and methylcyclohexane for the production of polybutadiene rubber, and styrene butadiene. A local group, Rubbertown Emergency Action, had fought the change, saying too little was known about the alternative chemicals. The air district disagreed. The company said the change would provide them flexibility to produce different rubber products, while reducing potential environmental impact.
Source: http://blogs.courier-journal.com/watchdogearth/2011/11/29/american-synthetic-rubber-co-can-change-chemicals/

4. *November 29, WLBT 3 Jackson* – (Mississippi) **Interstate 20 in Pearl re-opened.** Officials in Rankin County announced shortly after 4 a.m. November 29 that Interstate 20 in Pearl, Mississippi was back open following a November 28 spill of hazardous chemicals. A Pearl police lieutenant said clean up would continue throughout the morning. A portion of I-20 was shut down after several hundred gallons of hydrochloric acid were spilled inside R and L Trucking Lines at Becknell Drive and

Childre Road. Two businesses, the Bass Pro Shop and Sam's Club, were evacuated and road closures were ordered. Police closed the interstate from Pearson Road to Highway 49. The spill occurred when a large container of acid fell off a forklift, the police lieutenant said. He said 250 to 500 gallons of acid spilled. The Mississippi Department of Environmental Quality responded, and was overseeing the cleanup.
Source: http://www.wlbt.com/story/16141781/interstate-20-in-pearl-re-opened

5. *November 28, U.S. Environmental Protection Agency* – (National) **EPA releases formerly confidential chemical information.** To increase transparency, the U.S. Environmental Protection Agency (EPA) announced November 28 it was making available to the public hundreds of studies on chemicals previously treated as confidential business information (CBI). The newly available data on chemicals manufactured and processed in the United States can be found using the EPA's Chemical Data Access Tool. Since 2009, 577 formerly confidential chemical identities are no longer confidential, and more than 1,000 health and safety studies previously unavailable, or only available in limited circumstances are now publicly accessible. In 2010, the EPA issued guidance outlining plans to deny confidentiality claims for chemical identities in health and safety studies under the Toxic Substances Control Act determined to not be entitled to CBI status. The agency also asked companies to voluntarily relinquish CBI claims. To date, more than 35 companies have agreed to review previously submitted filings containing health and safety studies and determine if CBI claims may no longer be necessary. The newly available information can be found under a new "declassified tab" using the Chemical Data Access Tool, launched in December 2010.
Source: http://www.environmental-expert.com/news/epa-releases-formerly-confidential-chemical-information-269339

6. *November 28, WISN 12 Milwaukee* – (Wisconsin) **One worker dies, another injured in chemical spill at Theresa plant.** A 55-year-old man died following some type of chemical spill November 28 at a manufacturing plant in Theresa, Wisconsin, according to the Dodge County sheriff. A 65-year-old man was taken by ambulance to a hospital; he was in critical condition. The sheriff said the 65-year-old man's wife found the two men unconscious at about 3:45 p.m. at Vivid Image Inc., located at Highway 28 and County highway TW. Rescue crews said the victims were the only two employees at the plant. A haz-mat team was called out to deal with what authorities believe was a glue-type material that accidentally mixed with something else, creating deadly fumes. Rescue crews who responded and their gear had to be decontaminated. Officials indicated the medical examiner would not be able to perform an autopsy until November 29 because of chemicals on the victim's body.
Source: http://www.wisn.com/r/29874067/detail.html

For another story, see item 7

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

7. *November 28, U.S. Department of Labor* – (Wisconsin) **U.S. Labor Department's OSHA cites Northern Steel Castings in Wisconsin Rapids, Wis., for exposing workers to respiratory hazards.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) November 28 cited Northern Steel Castings Inc. for two safety and four health violations at its Wisconsin Rapids, Wisconsin, carbon steel foundry, including for overexposing workers to crystalline silica, a known respiratory hazard. Proposed fines total $95,480. The OSHA initiated the inspection after receiving a complaint alleging overexposure to crystalline silica. Breathing crystalline silica dust can cause silicosis, an incurable condition that reduces the ability of lungs to take in oxygen. The inspection found workers were overexposed to crystalline silica and one willful safety violation was cited. The company was also cited for two repeat health violations and three serious health violations, including overexposure to iron oxide and copper fumes, and failing to provide ventilation when welding.
Source: http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21369

[Return to top]

Defense Industrial Base Sector

8. *November 29, Associated Press* – (Mississippi) **Subcontractor owes Navy for stolen tools.** A 61-year-old man was fined $1,000 and ordered to repay the U.S. Navy nearly $5,000 for tools stolen while he worked as a civilian subcontractor at the Seabee Base in Gulfport, Mississippi, the Associated Press reported November 29. The Biloxi Sun Herald reports the man will also be on probation 3 years as part of a plea agreement to a charge of theft of government property. A U.S. attorney said the man stole the tools while he worked at the auto-body repair shop at the Naval Construction Battalion Center's construction equipment division. Court papers show the tools were taken between October 1, 2001, and July 31, 2008. The man pleaded guilty August 25, and was sentenced November 22. The judge ordered restitution of nearly $5,000.
Source: http://www.canadianbusiness.com/article/59252--subcontractor-owes-navy-for-stolen-tools

9. *November 28, FoxNews.com* – (Michigan) **17 suspended from plant that makes military parts after video allegedly shows workers drinking, smoking marijuana.** Seventeen workers from the Tower Defense and Aerospace plant in Detroit

have reportedly been suspended after an undercover investigation showed them smoking what appeared to be marijuana during their lunch break. Fox affiliate WJBK 2 Detroit released exclusive footage the week of November 21 showing several of the plant's workers allegedly drinking alcohol and smoking marijuana cigarettes while on a break. The plant reportedly manufactures armored parts for U.S. military trucks and planes, including parts for Humvees and Stryker combat vehicles to be sent to Afghanistan and Iraq. After the station's report, officials from the plant said in a statement that 17 of its employees have been "suspended pending discharge."
Source: http://www.foxnews.com/us/2011/11/28/17-suspended-from-plant-that-makes-military-parts-after-video-allegedly-shows/

[Return to top]

Banking and Finance Sector

10. *November 29, BankInfoSecurity* – (California) **Fraud scheme hits grocer.** Modesto, California-based grocery chain Save Mart Supermarkets issued a consumer advisory November 23 about card-reader breaches at 20 of its stores. According to a statement posted on Save Mart's Web site, tampered card-readers at self-service checkout lanes in 19 Lucky Supermarkets locations and one Save Mart store were discovered during routine maintenance. The statement did not say when the tampering might have occurred or what method of tampering was used. It is not clear if skimmers were installed, or if the card readers were replaced with readers manipulated to collect details. Save Mart did say, however, that it replaced readers on all of the affected terminals and added additional security to point-of-sale card readers in all of its 234 locations soon after the tampering was discovered. "We are not aware nor have we been notified of any reports that customer accounts were compromised," the company statement said. "The appropriate authorities have been notified of this situation and consumer notices have been posted at credit/debit terminals in the affected stores as well as placed on our Web sites."
Source: http://www.bankinfosecurity.com/articles.php?art_id=4280

11. *November 28, CNN* – (National) **Citigroup's mortgage securities fraud settlement with SEC rejected.** A judge rejected a proposed $285 million mortgage securities fraud settlement between Citigroup and the Securities and Exchange Commission (SEC) November 28, saying the deal was "neither fair, nor reasonable, nor adequate, nor in the public interest." A judge said that the settlement announced in October 2011, under which Citi neither admitted nor denied the SEC's allegations, deprived the public "of ever knowing the truth in a matter of obvious public importance." He instead ordered Citi to face trial over the allegations in July 2012. A spokeswoman for Citi said the bank was "declining to comment, pending a review of the decision." The SEC has alleged that in 2007, Citi created and sold a mortgage-related collatarized debt obligation, or CDO, called Class V Funding III. After marketing the CDO, Citi then took a short position — or bet against — the security as the housing market deteriorated, bringing in a net profit of $160 million for the bank. Investors, meanwhile, lost more than $700 million.

Source: http://www.chicagotribune.com/business/breaking/chi-citigroups-mortgage-securities-fraud-settlement-with-sec-rejected-20111128,0,5534190.story

12. *November 28, WDEF 12 Chattanooga* – (Georgia) **Debit card scam not linked to any local retailers.** Hundreds of north Georgia residents found themselves in the middle of a scam the week of November 21. Officials believe the scam started November 23, when many Walker County residents found themselves with a depleted bank account. "We've seen charges made from people's card from Spain to Egypt to Europe to Mexico," a LaFayette Police Department sergeant said. Officials believe this is an elaborate crime ring that used the holiday to take advantage of people's accounts. "We have not tracked this source back to any particular business in our jurisdiction. I can tell you that with absolute certainty," the sergeant said. Officials said about 400 to 500 residents have reported the issue to local banks in the Walker County and LaFayette area. There has also been reports of the same scam in other counties. "There could be as many as 100 victims in the Chattooga County area," the Walker County sheriff said. Officials said the scam starts with the credit card processing company, not a local retailer. The FBI is assisting in the investigation.
Source: http://www.wdef.com/news/story/Debit-Card-Scam-Not-Linked-To-Any-Local-Retailers/-hTdSz-59kC2wPBqNRpFYw.cspx

13. *November 28, Grand Rapids Press* – (Michigan) **Grand Rapids-area broker described as 'mini-Madoff' in alleged Ponzi scheme.** A Grand Rapids, Michigan stockbroker is facing federal allegations linked to a $6-million Ponzi-style scheme, the Grand Rapids Press reported November 28. The government has filed felony information accusing the broker of mail fraud for sending falsified account statements to clients. The U.S. Securities and Exchange Commission (SEC) earlier filed a civil injunction against the broker and his companies, Wealth Resources Inc. and Wealth Resources LLC, alleging he acted as an unregistered broker and investment adviser to raise funds from at least 20 investors. "Based upon representations made by [the broker] investors gave money to [the man] to place in Wealth Resources LLC and invest on their behalf," an assistant U.S. attorney wrote in court documents. "[He] induced his clients to withdraw money from their retirement accounts, investment accounts, bank accounts and from other sources on the premise that [he] would invest their money into legitimate investment opportunities. However, [he] lied about the success of Wealth Resources LLC, and other investment opportunities that he recommended, and diverted some of his clients' money for his own use." The attorney said he "fabricated" account statements that led "clients to believe that their investment was safe and growing." The broker was a registered representative of New England Securities from December 1998 to April 2010. When the broker filed for bankruptcy in June 2010, clients filed a complaint to prevent discharge of his $4.3 million debt to them, court records showed. The government said he used some of the money to "make Ponzi-like payments to other customers who requested a return of all or part of their investment."
Source: http://www.mlive.com/news/grand-rapids/index.ssf/2011/11/grand_rapids-area_broker_descr.html

14. *November 28, Fort Worth Star-Telegram* – (Texas) **2 UNT freshmen accused of printing fake money in dorm.** Two University of North Texas freshmen were arrested November 7 on suspicion of forgery, and accused of running a counterfeiting operation from a dorm room until a store clerk reported receiving a fake $20 bill to Denton, Texas, police. Denton officers arrested the students after an officer found fake $1 and $20 bills atop a printer in one of their dormitories, police said. The students face a felony charge of forgery, which carries a sentence of 180 days to 2 years in state jail, and a fine of up to $10,000. The case came under police scrutiny when a convenience store clerk reported a questionable-looking $20 bill, a Denton police spokesman said. The investigation led to a search of a student's dorm room which turned up a scanner/printer, and a computer used to print money. "Apparently there was money on top of it that they were still in the process of making money," the Denton police spokesman said. He said the counterfeit bills were passed at area fast-food restaurants and convenience stores.
    Source: http://www.star-telegram.com/2011/11/28/3556376/2-unt-freshmen-accused-of-printing.html#storylink=omni_popular

15. *November 23, Federal Bureau of Investigation* – (National) **FBI Denver Cyber Squad advises citizens to be aware of a new phishing campaign.** The FBI Denver Cyber Squad advised citizens of a new spear phishing campaign involving personal and business bank accounts, financial institutions, money mules, and jewelry stores. The campaign involves a variant of the "Zeus" malware called "Gameover." The campaign features e-mails claiming to be from the National Automated Clearing House Association (NACHA), and advising the user of a problem with an ACH transaction at their bank that was not processed. Users that click on the link are infected with the Zeus or Gameover malware, which can key log as well as steal online banking credentials, defeating several forms of two-factor authentication. After accounts are compromised, the perpetrators conduct a Distributed Denial of Service (DDoS) attack on the financial institution. The belief is the DDoS is used to deflect attention from the wire transfers as well to prevent a reversal of the transactions (if found). A portion of the wire transfers is being transmitted directly to high-end jewelry stores, wherein the money mule comes to the actual store to pick up his $100,000 in jewels (or whatever dollar amount was wired). An investigation has shown the perpetrators contact the high-end jeweler requesting to purchase precious stones and high-end watches. The perpetrators advise they will wire the money to the jeweler’s account and someone will come pick up the merchandise. The next day, a money mule arrives at the store, the jeweler confirms the money has been transferred or is listed as "pending" and releases the merchandise to the mule. Later on, the transaction is reversed or cancelled (if the financial institution caught the fraud in time), and the jeweler is out whatever jewels the money mule was able to obtain.
    Source: http://www.fbi.gov/denver/press-releases/2011/fbi-denver-cyber-squad-advises-citizens-to-be-aware-of-a-new-phishing-campaign?utm_campaign=email-Immediate&utm_medium=email&utm_source=denver-press-releases&utm_content=51037

For another story, see item **38**

[Return to top]

Transportation Sector

16. *November 29, Mid-Hudson News Network* – (New York) **Port Jervis Line commuters return for first day of full service.** In New York, commuters returned to Metro-North's Port Jervis Line November 28 for the first time since August, when 14 miles of the track were ravaged by Tropical Storm Irene. Full service has been restored with 26 trains running daily and 14 trains each weekend day, though traveling times have been slightly extended to provide for ongoing work. Along with repairs, Metropolitan Transportation Authority (MTA) workers have and will continue to install countermeasures to prevent flood damage in the future, including slope protection, drainage and piping structures, as well as riprap in sections that tend to washout. The line will return to its pre-storm schedule January 15, 2012. Repairs included thousands of feet of washed out track being resurfaced using fill and ballast, requiring about 150,000 tons, as well as the installation of several new culverts. According to the MTA, the $30 million to $40 million in repairs landed well short of the $60 million expected -- and finished a month earlier than expected.
Source: http://www.midhudsonnews.com/News/2011/November/29/PJ_train_restore-29Nov11.html

17. *November 28, Inland Valley Daily Bulletin* – (California) **Man arrested after throwing stars found in carry on.** A man was arrested November 28 for allegedly carrying martial arts throwing stars in his carry-on bag at Ontario International Airport in Ontario, California. Transportation Security Administration (TSA) officers found four throwing stars in the suspect's bag while he was being screened at Terminal 4, according to a TSA news release. The man, whose name was not released, was bound for Phoenix before he was arrested. Martial arts and self-defense weapons are prohibited from carry-on baggage, said a TSA spokesman, but some of those items can be transported in checked baggage. The suspect is subject to penalties in addition to the arrest, officials said. He could face up to $1,500 in fines.
Source: http://www.dailybulletin.com/ci_19428239

18. *November 28, NY1 News* – (New York) **Local airports confiscate dangerous weapons over Thanksgiving weekend.** Transportation Security Administration (TSA) officials showed off dangerous weapons confiscated at area airports over the Thanksgiving holiday weekend. Port Authority of New York and New Jersey police arrested a man bound for the Dominican Republic November 26 after screeners at John F. Kennedy International Airport in Queens, New York found a combination brass knuckles and knife in his checked bag. They also nabbed a man who they said was headed to Germany from Newark Liberty International Airport in Newark, New Jersey with a set of brass knuckles in his carry-on bag. On November 27, authorities took a man into custody after they said he tried to carry a butterfly knife on board a plane at LaGuardia Airport in Long Island, New York.
Source: http://www.ny1.com/content/news_beats/transit/151523/local-airports-confiscate-dangerous-weapons-over-thanksgiving-weekend

For more stories, see items **1**, **4**, **28**, and **47**

[Return to top]

Postal and Shipping Sector

19. *November 28, Computerworld* – (National) **Criminals sabotaging Cyber Monday, security experts warn.** Security experts November 28 warned consumers of a rapidly mutating spam campaign using bogus messages from United Parcel Service (UPS) claiming a package could not be delivered. The spam run, which actually began earlier in November, is just one way security researchers believe criminals will exploit the holiday season online buying spree. According to Cloudmark's engineering director, the UPS-based scam uses phony e-mail to dupe recipients into opening an attachment or clicking on a link to infect machines with malware. "We've seen a number of variants ... some with attachments, some with no attachments and bad links, all of them personalized to the recipient, and sent from an ever-changing list of fake UPS employees or the generic 'UPS Customer Services,' " said the director in a blog post November 28. The attached files are .zip archives that contain malware, he said, while the links lead to compromised or hacker-controlled Web sites. Experts urged users — both at home and at work, where many shop using their office's faster Internet connection — to be wary of fake sites and too-good-to-be-true discounts pitched via e-mail and social media. SecureWorks also encouraged users to ensure their browsers and browser plug-ins, especially document viewers such as Adobe Reader, abd music, and video player utilities like Flash, are up to date with the most recent security patches.
Source: http://www.computerworld.com/s/article/9222209/Criminals_sabotaging_Cyber_Monday_security_experts_warn

[Return to top]

Agriculture and Food Sector

20. *November 29, Food Safety News* – (California) **Allergen alert: British-style sausages.** Silva Sausage Co. of Gilroy, California is recalling about 1,010 pounds of British-style "banger" sausages because of misbranding and an undeclared allergen, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced November 28. The pork sausages contain wheat, a known allergen, which is not noted on the label. The FSIS discovered the problem during a label review, and it is believed that wheat was left off the label when the company changed its in-house label printing program. The recall involves 10-pound cases of Silva Sausage English Brand Bangers. The sausages were distributed for institutional use in Livermore, and Sacramento, California.
Source: http://www.foodsafetynews.com/2011/11/allergen-alert-british-style-sausages/

21. *November 29, Food Safety News* – (National) **Smoked salmon recalled for Listeria concerns.** Trans-Ocean Products of Bellingham, Washington is recalling its 4-ounce "transOCEAN Wild Alaska Sockeye Smoked Salmon" because the fish may be

contaminated with Listeria monocytogenes, Food Safety News reported November 29. Trans-Ocean Products did not produce the product and the potential for contamination was reported by the manufacturer. Distribution of the product has been suspended while the U.S. Food and Drug Administration and Trans-Ocean Products investigate the source of the problem. The recalled packages were distributed to four supermarket chains in six states: Demoulas Marketbasket in Massachusetts and New Hampshire; Giant Eagle in Pennsylvania, West Virginia, Maryland, and Ohio.
Source: http://www.foodsafetynews.com/2011/11/smoked-salmon-recalled-for-listeria-concerns/

22. *November 29, Food Safety News* – (National) **Canned pumpkin recalled by Giant Eagle.** Saying the product does not meet unspecified "quality standards," Giant Eagle grocery chain has recalled Valu Time brand canned pumpkin purchased on or after August 30 and Food Club brand canned pumpkin purchased on or after October 28, Food Safety News reported November 29. Those brands are produced by Topco Associates. Giant Eagle said it is "working with Topco to further investigate the situation and will notify customers if any additional actions are warranted as a result of these efforts." Giant Eagle also said it was "not aware of any immediate health concern," but added "customers should not consume these products in any way, or anything in which they were used as ingredients, and should dispose of the product."
Source: http://www.foodsafetynews.com/2011/11/canned-pumpkin-recalled/

23. *November 28, Associated Press* – (National) **Army Corps to return Asian carp barrier to higher voltage after month-long tests.** The U.S. Army Corps of Engineers announced November 28 it is restoring a higher power setting on an electric barrier designed to prevent Asian carp and other fish from using a Chicago-area waterway to migrate between the Great Lakes and Mississippi River systems. The Corps announced in October it was ramping up the juice in the barrier about 37 miles by water from Lake Michigan. But shortly afterward, power was reduced to its previous level because of concerns it affected signals on a nearby railroad. Investigators identified a piece of equipment causing the problem and reconfigured it, the Corps said. The barrier was scheduled to be returned to the higher setting November 29. The barrier is one of three in the Chicago Sanitary and Ship Canal, part of a man-made waterway linking Lake Michigan to the Mississippi basin. The canal could provide a pathway to the Great Lakes for the large, voracious carp. Scientists said if allowed to gain a foothold in the lakes, the carp could destabilize the food chain and damage the $7 billion fishing industry. The Corps boosted the power level in October from 2 volts per square inch to 2.3 volts and also intensified the duration and frequency of pulses after research questioned whether the force field was strong enough to stop tiny fish. Officials said baby Asian carp had been observed in spawning areas more than 150 miles from Lake Michigan, but were not believed to be near the electric barrier. Scientists have detected Asian carp DNA beyond the barrier. But the Corps said it has tagged numerous fish in the area and none have swum upstream through the electric field.
Source: http://www.chicagotribune.com/news/local/breaking/chi-army-corps-to-return-asian-carp-barrier-to-higher-levels-after-monthlong-tests-20111128,0,2981573.story

24. *November 28, Indiana Public Media* – (Indiana; South Dakota) **Cows quarantined after possible tuberculosis exposure.** The Indiana State Board of Animal Health said it quarantined several cattle herds that might have been exposed to bovine tuberculosis, Indiana Public Media reported November 28. The agency said it was notified by the South Dakota State Veterinarian that seven head of beef cattle recently shipped to Indiana may have been exposed to the chronic bacterial disease. The agency said it has identified all of the herds to which the South Dakota cattle were shipped. None of the imported cattle have tested positive for the disease.
Source: http://indianapublicmedia.org/news/cows-quarantined-tuberculosis-exposure-24048/

25. *November 28, Food Safety News* – (International) **80 ill after charity dinner at British hotel.** Chicken pate has been implicated as the possible source of an outbreak of foodborne illness that sickened 80 guests following a fundraising dinner at the luxury Lowry Hotel near Manchester, England, Food Safety News reported November 28. According to a story in the Daily Mail, lab test have confirmed that a number of the guests who reported symptoms of dizziness, fever, and vomiting were infected by Campylobacter. A consultant with the UK's Health Protection Authority, told the newspaper the investigation is continuing, including analysis of a food-history questionnaire returned by the guests. About 200 people attended the charity function.
Source: http://www.foodsafetynews.com/2011/11/80-ill-after-charity-dinner-at-british-hotel/

For more stories, see items **10** and **14**

[Return to top]

Water Sector

26. *November 29, San Francisco Chronicle* – (California) **Officials probe water main burst in South S.F.** Utility officials continued to investigate why a water main broke November 25 in a South San Francisco neighborhood, creating a 60-foot geyser that spilled more than a million gallons of water and damaged homes, cars, and other property. The San Francisco Chronicle reported the cause of the break is not expected to be determined for days, but officials from the San Francisco Public Utilities Commission acknowledged that the pipe segments involved were upgraded and put back into service about 2 weeks ago as a part of the Hetch Hetchy water system retrofit project. A minor leak, reported November 25, turned into a major geyser about an hour later, an official said. The force of the water prevented crews from getting within 20 feet of the rupture, but workers were able to start closing off two water valves located 4 miles apart a few hours later. Between 1 million and 2 million gallons of water poured into the neighborhood before the water was totally shut off at 12:55 p.m. Residents near the rupture were evacuated, but all were allowed to return to their homes by the evening.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/11/28/BA1K1M573O.DTL

27. *November 29, Fredericksburg Free Lance-Star* – (Virginia) **Pump failure sends sewage into river.** Fredericksburg, Virginia, officials are still unsure why a pump station malfunctioned, sending a "significant" amount of raw sewage into the Rappahannock River the week of November 21. The public works director said the problem was discovered November 22 when an alarm was detected at the station. Both pumps, one primary and one backup, were down because of an apparent electrical problem, he said. There are eight sewage pump stations in the city. The director was unable to say how much sewage, bound for the Fredericksburg Wastewater Treatment Plant, spilled into the river. Samples returned on November 25 indicated higher levels of fecal coliform around the City Dock. The latest results were expected November 30. The director said testing would continue "until we are confident that everything has cleared back up." The spill was reported to the Virginia Department of Environmental Quality, which is reviewing the incident.
Source: http://fredericksburg.com/News/FLS/2011/112011/11292011/667588

28. *November 29, KGTV 10 San Diego* – (California) **Linda Vista water main break repaired.** A water-main break left about 50 homes in the Linda Vista section of San Diego, without working plumbing for more than 11 hours November 28. The ruptured 6-inch-diameter cast-iron pipeline began inundating the roadway shortly before 1 a.m., according to the San Diego Water Department (SDWD). It took crews about 2 hours to halt the overflow, which sent "a lot" of mud cascading down the sloping road, a SDWD spokesman said. Outside of cracked and collapsed street pavement, no property damage was reported, he said. The city sent in two "water wagons" to serve the affected residents pending repairs, which were complete by 12:15 p.m., according to officials.
Source: http://www.10news.com/news/29874186/detail.html

[Return to top]

Public Health and Healthcare Sector

29. *November 28, Topeka Capital-Journal* – (Kansas) **Salina nurse pleads guilty to stealing morphine.** A Salina, Kansas, nurse who was addicted to painkillers pleaded guilty to stealing morphine from the nursing facility where she worked, a U.S. attorney for Kansas said November 28. In her plea, she admitted that in May 2009 she was fired from Wesley Medical Center for taking Percocet from the hospital's drug supply without a physician's order and without documenting she administered it to a patient. In August 2009, she went to work as a charge nurse at Holiday Resort Nursing Facility in Salina. Because she was addicted to pain medications, she took syringes from the medical room, removed morphine from its vials and replaced it with sodium chloride solution to hide the theft. She would take the morphine-filled syringes home and inject the morphine. In February 2010, a nursing director was preparing an injection for a patient and discovered that someone had tampered with multiple vials. The nursing director had her submit to a urine drug test, which was positive for opiates.
Source: http://cjonline.com/node/111244

For another story, see item **30**

[Return to top]

Government Facilities Sector

30. *November 29, BBC* – (International) **United Nations agency 'hacking attack' investigated.** A group of hackers posted more than 100 e-mail addresses and log-in details it claimed to have extracted from the United Nations. Many of the e-mails involved appear to belong to members of the United Nations Development Programme (UNDP). The group, which identifies itself as Teampoison, attacked the UN's behavior and calledit a "fraud". A spokeswoman for the UNDP said the agency believed "an old server which contains old data" had been targeted. "UNDP is taking action to close any vulnerabilities on our Web site," she said. "Please note that UNDP.org was not compromised." The details were posted on the Web site Pastebin under the Teampoison logo. Many of the e-mail addresses gend in undp.org, but others appear to belong to members of the Organization for Economic Cooperation and Development, the World Health Organization, and the United Kingdom's Office for National Statistics. The poster noted that several of the accounts had "no passwords".
Source: http://www.bbc.co.uk/news/technology-15951883

31. *November 28, KSTP 5 St. Paul* – (Minnesota) **Student recovering after chemical incident at New Hope Playground.** A New Hope, Minneapolis, elementary school student is expected to return to school November 29 after a water bottle containing a mix of ammonia and other chemicals exploded in her face on the playground November 28. A district spokesperson said the child found the bottle on the playground at Meadow Lake Elementary. Officials said ite contained a mix of chemicals that spewed out when opened. The child was transported to the hospital, and was treated and released. School officials immediately cleared the playground and alerted authorities after the incident. Police found another similar bottle during a sweep of the area. They are now reviewing video tapes of the playground to figure out who put the bottles there.
Source: http://kstp.com/news/stories/S2390032.shtml?cat=1

For more stories, see items **8**, **9**, **14**, and **34**

[Return to top]

Emergency Services Sector

32. *November 28, NextGov* – (National) **Cellphone emergency call service failed following East Coast quake.** A cellphone service that is supposed to grant priority to emergency government and public safety calls failed during the August earthquake that rocked the East Coast, a DHS official said November 28. The Wireless Priority Service, a voice feature that does not require a special cellphone, was overwhelmed by text-messaging traffic in the aftermath of the 5.8 magnitude shaker August 23, said the acting director of the DHS National Communications System. It is widely acknowledged that many Americans were unable to make personal calls for several minutes following the earthquake. DHS officials are working with carriers to modify

their circuitry by the time of the Republican and Democratic national conventions late summer of next year, he said. "That is a significant requirement that we must have," he said. He told Nextgov that Alcatel-Lucent's hardware should be fixed by Christmas.
Source: http://www.nextgov.com/nextgov/ng_20111128_2122.php

33. *November 28, KCRA 3 Sacramento* – (California) **Stockton fire crews battle two-alarm fire.** Stockton, California fire crews were working November 28 to gain control of a fire inside a warehouse containing vinyl glass windows. Fire investigators said the two-alarm fire started shortly after 8:30 p.m. San Joaquin County Sheriff's deputies said they were called to the scene because several people were attempting to steal fire equipment off the fire trucks while firefighters battled the blaze. Investigators said there was no chemical threat to neighbors since the wind was blowing the fumes away from homes in the area. The cause of the fire is under investigation.
Source: http://www.kcra.com/r/29876362/detail.html

34. *November 28, Associated Press* – (North Dakota) **150 Fargo jail inmates sickened, possbily from food poisoning.** Health officials are investigating whether food poisoning caused more than 150 inmates at the Cass County Jail in Fargo, North Dakota, to get sick. The Cass County sheriff said November 28 that inmates began showing flu-like symptoms after their November 27 meal, which included a casserole made of chili, ground turkey, and macaroni, corn, cornbread, whipped margarine, cookies, and a powdered drink. No inmates were hospitalized and most were feeling better by the afternoon of November 28, he said. The chief nurse at the jail said most of the inmates were being treated with fluids. The sheriff said the investigation will look into whether the illness was a result of an intentional act or if it was caused by something other than tainted food. Some inmates help prepare the food, but are closely monitored by staff members, the sheriff said.
Source: http://www.twincities.com/ci_19427158

[Return to top]

Information Technology Sector

35. *November 29, The Register* – (International) **13 million gamers in ID theft scare after Nexon breach.** An estimated 13 million gamers have been left at greater risk of ID theft following a breach at gaming firm Nexon. Data including names, usernames, encrypted resident registration numbers, and password hashes was exposed as a result of the breach at Nexon, which maintains the popular online role-playing game, Maple Story. The data breach followed a hack on a backup server for Maple Story late the week of November 21. Details of the 5 million customers of other games maintained by Nexon were not exposed. Nexon promised to bolster its security in the wake of the attack, the Korean Herald reports. In addition, it is offering game items to gamers who change their passwords.
Source: http://www.theregister.co.uk/2011/11/29/nexon_data_breach/

36. *November 29, Softpedia* – (International) **HP printers may be remotely set on fire, researchers say.** Researchers at Columbia University in New York City found a HP

LaserJet printer vulnerability that could allow a hacker to remotely control the device to launch cyberattacks, steal data that is being printed, and even instruct its mechanical components to overload until it catches fire. According to MSNBC, the researchers revealed the flaw they found does not affect only HP printers, but also other devices utilized by millions of individuals and companies that so far were considered to be safe. In the case of the HP printers which they thoroughly tested, the researchers relied on the fact remote software updates are not checked for signatures or certificates when they are being installed. In another demonstration, by sending a specially crafted print job, they were able to inject a code that would automatically scan printed documents for sensitive information, transmitting the data to a Twitter feed. They showed an infected computer could instruct the printer's fuser, the one used to dry off the paper, to continuously heat up until the device self-destructs or, if it lacks a fuse, to set itself on fire. They also proved a hijacked printer could act as a gate-opener for a full-effect attack on a company network. They even made a demo from computers running Mac and Linux operating systems. HP representatives argue the situation might not be all that disastrous, claiming their newer models check for signatures while performing firmware updates. However, they are currently investigating the issue to determine exactly what is affected and what can be done about it. Even though later printer models should be more secure, the researchers claim one of the printers used in their tests was purchased not long ago.
Source: http://news.softpedia.com/news/HP-Printers-May-Be-Remotely-Set-On-Fire-Researchers-Say-237254.shtml

37. *November 29, Softpedia* – (International) **Russian spammers rely on new techniques to mask phone numbers.** Some spam messages contain phone numbers instead of links that point to locations where different products are advertised. To make sure they successfully avoid spam filters, Russian spammers devised new ways to keep phone numbers secret. Symantec researchers reveal the large number of methods utilized by Russian spammers to list phone numbers in e-mail messages without raising the suspicion of any anti-spam solution. One of the simpler methods implies placing symbols between the figures that compose the number. In some cases, Russian characters that resemble figures will be utilized to replace some numbers. Also, in some scenarios, the numbers were actually spelled in Russian words. One final strategy involves writing the area code with the actual name of the city it represents.
Source: http://news.softpedia.com/news/Russian-Spammers-Rely-on-New-Techniques-to-Mask-Phone-Numbers-237269.shtml

38. *November 29, The Register* – (International) **Danger worm hijacks Facebook accounts to inject banking trojan.** A dangerous worm is using Facebook to spread itself by posting malicious links on the social networking Web site that point to malware-tainted sites loaded with a variant of the Zeus banking trojan as well as other pieces of malware. The malware uses stolen Facebook account credentials to log into compromised accounts and post links, according to security researchers at CSIS in Denmark, who were the first to detect the threat. The malicious links generated by the worm pose as links to a photo file posted by the account-holder's friend or online acquaintance. In reality, the file is a booby-trapped screensaver file with a .jpg file extension. Users have to download and open the file but if tricked into doing so, the

consequences can be serious –- especially since anti-virus detection rates are quite low. CSIS added the worm is also using other domains to spread.
Source: http://www.theregister.co.uk/2011/11/29/facebook_worm_spreads/

39. *November 29, Help Net Security* – (International) **FakeScanti rogue sends users to download additional fake AV solution.** The Blackhole exploit kit has been getting a lot of attention recently, because it is continually updated with exploits for various flaws in popular software, and can deliver practically any malware the attackers want it to. Among those malware are rogue AV solutions such as those belonging to the FakeScanti malware family. One of the variants — named "AV Protection 2011"— can modify the infected computer's HOSTS file (the file that allows the system to connect hostnames to IP addresses) so that when the user tries to visit the Google Search engine, Facebook, or Bing, he/she is redirected to a page hosted in Germany that serves up another variant of the same family. The hijacking of the HOSTS file is not unusual behavior when it comes to worms and backdoors, but it not often seen in rogue AV solutions, said a GFI researcher. The technique is also often used by phishers for seamlessly redirecting users to phishing pages when they try to visit legitimate ones.
Source: http://www.net-security.org/malware_news.php?id=1920

40. *November 28, H Security* – (International) **Google+ security attracts praise and criticism.** Security researchers at University College London subjected Google+ to a first IT security analysis, the main focus of which was on privacy. The currently preliminary results are ambivalent: the researchers commended new functions which improve networking security among friends, but they have also highlighted several potentially problematic details. Among these concerns is the way in which Google+ currently handles images. The researchers showed that photos uploaded to the network retain their metadata. However, they say the service does not inform users about this. Another problem area is the Google+ "About" section. There, Google is apparently prompting users to list previous addresses, previous names, and their maiden name. The researchers said this information could be particularly useful to identity thieves. The researchers commended the fact that Google+ uses SSL encryption by default, for the entire Google+ network connection. Facebook only uses this encryption for its lo-gin page, unless a user explicitly enables the security feature. The researchers concluded that, therefore, Google+ sessions offer better protection against "man-in-the-middle" attacks.
Source: http://www.h-online.com/security/news/item/Google-security-attracts-praise-and-criticism-1386437.html

For more stories, see items **15**, **19**, and **30**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

41. *November 28, Internet Retailer* – (National) **The Thanksgiving weekend brings site headaches for multiple online retailers.** PC Mall Inc. and Crutchfield Corp. were among the retailers experiencing significant downtime on their e-commerce sites November 28, according to Web site, performance-monitoring firm Catchpoint Systems Inc. The e-commerce site operated by PC Mall had suffered 77 minutes of downtime as of noon Eastern time, Catchpoint said. The Crutchfield site had 60 minutes of downtime. Other e-commerce site also experienced problems over the holiday weekend, according to a report from Web site performance monitoring firm AlertBot. The site operated by American Eagle Outfitters Inc. was down for a little over 8 hours between about 9 p.m. Eastern time November 23 and November 28, an AlertBot sales and marketing manager said. "An error message appeared numerous times over the Thanksgiving break," he said. The e-commerce site operated by Target Corp. experienced loading problems for more than 2 hours November 25, the day after Thanksgiving — the latest difficulty for the redesigned site since its introduction in August. The problems occurred between 3:30 p.m. and 4:10 p.m. and 5:10 p.m. and 6:45 p.m. Eastern time November 25, AlertBot said.
    Source: http://www.internetretailer.com/2011/11/28/thanksgiving-weekend-brings-multiple-site-headaches

For more stories, see items **32**, **38**, and **40**

[Return to top]

Commercial Facilities Sector

42. *November 29, York Daily Record* – (Pennsylvania) **Children critically injured after car crashes into toy section of thrift store.** Two children who were playing in the toy section of a thrift store in Maxatawny Township, Pennsylvania were critically injured when a car crashed into the store November 28, officials said. The children were in Once Again Thrift Store when a woman who was parking her car thought she hit the brake, but the car jumped the sidewalk and crashed into the store, Berks-Lehigh Regional police said. The children were taken to the hospital. Both were in critical condition late November 28, hospital officials said. Officials said the car smashed through the front of the store and continued on a roughly 45-degree angle over the tile floor to the toy section, striking the children, and coming to rest against a mirrored wall.
    Source: http://www.ydr.com/ci_19428145

43. *November 29, Oakland Tribune* – (California) **At least eight shot including 1-year-old child in West Oakland.** At least eight people, including a 1-year-old boy, were shot late November 28 in Oakland, California during what police said was a videotaping of a rap music video. The child was reported in critical condition after undergoing surgery for a bullet wound to the head. An adult woman was also in critical

condition with unspecified injuries, according to an Oakland police department spokeswoman. Police said the other victims were in stable condition. Police said an Oakland rapper was at the scene of the shooting, which happened in the parking lot of a liquor store where dozens of people had gathered. The spokeswoman said that at some point an argument erupted and bullets started flying. A van belonging to the rapper was riddled with gunshots, and at least 50 shell casings littered the parking lot.
Source: http://www.mercurynews.com/breaking-news/ci_19428949?source=autofeed#

44. *November 28, Detroit Free Press* – (Michigan) **Fires break out in six Detroit vacant homes.** Detroit Fire Department investigators are trying to determine who set six fires in vacant homes on the city's north side November 28. The first of four fires was reported at 3:50 a.m., an arson unit lieutenant said. Two more fires were reported, each a couple of blocks away, the last at 5:08 a.m. "We were at a different area on the west side last week, same thing," the lieutenant said. "It's suspicious. When you look at it geographically, it looks like it's someone walking down the street, setting fires in houses." Investigators are still trying to determine who set three fires set within 20 minutes of each other November 24 on the city's west side near Plymouth and Southfield. In the fires November 28, two of the homes burned and collapsed.
Source: http://www.firehouse.com/news/top-headlines/fires-break-out-six-detroit-vacant-homes

45. *November 28, WNWO 49 Toledo* – (Ohio) **Adrian apartments evacuated after meth lab fire.** A meth lab in an Adrian, Ohio apartment caused a fire and forced an evacuation November 26. It happened at the Carriage House Apartments. Police said when a man was mixing chemicals to make methamphetamines, a fire erupted. They said the man put the fire out in bathtub and tried to get rid of the evidence but was stopped by police. Hazmat crews were called to the scene and some apartments were evacuated while the hazardous materials were cleaned up.
Source: http://www.northwestohio.com/news/story.aspx?id=691374#.TtT4IFaLNqo

For more stories, see items **4**, **15**, **26**, **33**, **36**, **41**, and **46**

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

46. *November 28, Lancaster Intelligencer Journal* – (Pennsylvania) **Lake at Speedwell Forge gets a refill.** The 106-acre lake at Speedwell Forge in Elizabeth Township, Pennsylvania was drained in October, after officials with the Pennsylvania Fish & Boat Commission discovered cracks and fissures in the dam caused by recent storm activity, including Hurricane Irene and Tropical Storm Lee, the Lancaster Intelligencer Journal

reported November 28. The lake has refilled after clogging the weakened dam on Hammer Creek with debris, according to a nearby resident. The resident warned that, as the water continues to rise, the dam could break, flooding about 80 homes downstream. Hammer Creek feeds into the man-made lake from the north and flows southeast from the spillway in Elizabeth Township. Commission officials have said their hands are tied until funds for reconstruction of the dam — estimated at $6.3 million — are found. In the meantime, however, some remediation of the dam is necessary to prevent it from collapsing and flooding homes downstream on Hammer Creek. Engineers have already examined the site, a commission spokesman said, "and we're taking steps to clear the debris that's clogging it." A state senator said he contacted state and federal authorities about the abrupt rise in water levels. "There was no structural improvement to the dam, so I would conclude there is certainly a hazard there," he said. The commission, he noted, is working with the state department of environmental protection, and the state department of general services on the project.
Source: http://lancasteronline.com/article/local/506794_Lake-at-Speedwell-Forge-gets-a-refill.html

47. *November 27, Associated Press* – (Vermont) **Vermonters mull pluses, risks, of rerouting rivers after Irene.** Vermont residents are finding some rivers rerouted by the floodwaters of Tropical Storm Irene, and it is not clear whether putting them back on their original path is the best idea. The Burlington Free Press reported the issue has come up in several places. North of Rutland, the East Creek was clogged with mounds of debris some residents fear will cut off the road and threaten three dams and the Chittenden Reservoir with the next heavy rain. Local residents recently asked the governor to clear out the debris and fix the creek that Irene rerouted, however, a state river management engineer, urged caution. He said clearing the way in one spot could cause further damage downstream by increasing the river's flow.
Source:
http://www.therepublic.com/view/story/3332e4c3d901471a9c8f57528eb14965/VT--Rerouting-Rivers/

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

About the 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 Web site: http://www.dhs.gov/iaipdailyreport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

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