Daily Open Source Infrastructure Report
29 October 2012

Top Stories

- A Los Angeles-based accountant who admitted to participating in a $100 million mortgage fraud scheme by creating fake documents for straw buyers pleaded guilty October 25 to wire fraud. – *Courthouse News Service* (See item **6**)
- A New York City Police Department officer who allegedly used law enforcement databases to plan to kidnap, cook, and eat as many as 100 women was arrested following a joint NYPD and FBI investigation. – *ABC News* (See item **23**)
- The CoDeSys software tool used to manage equipment in power plants, military environments, and nautical ships contains an undocumented backdoor that could allow malicious hackers to access sensitive systems without authorization. – *Ars Technica* (See item **31**)
- Kentucky State Police searched for the suspect who called in several bomb threats in Monroe County, forcing evacuations at several businesses, schools, and government offices. – *WTVF 5 Nashville* (See item **32**)

Fast Jump Menu

Energy Sector

1. *October 25, Associated Press* – (Louisiana; International) **BP caps dome believed to be source of oil sheen.** October 25, BP said it capped and plugged an abandoned piece of equipment that is believed to be the source of a sheen spotted near the site of the 2010 oil spill in the Gulf of Mexico. The company said it successfully placed a 750-pound cap over an 86-ton steel container the company deployed in a failed effort to contain the spill. BP also inserted plugs on the top and sides of the container. BP and the Coast Guard both said no oil has been seen leaking out of the container since it was capped and plugged. The sheen appeared on the surface of the Gulf in September. BP plans to monitor the sheen by satellite for several more days.
   Source: http://www.kwwl.com/story/19915050/bp-caps-dome-believed-to-be-source-of-oil-sheen

[Return to top]

Chemical Industry Sector

See item **37**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

2. *October 26, Homeland Security News Wire* – (International) **Understanding the effects of Fukushima by studying fish.** A Woods Hole Oceanographic Institution (WHOI) release reported that in a "Perspectives" article in the October 26 issue of the journal Science, a WHOI marine chemist analyzed data made publicly available by the Japanese Ministry of Agriculture, Forestry, and Fisheries on radiation levels in fish, shellfish, and seaweed collected at ports and inland sites in and around Fukushima Prefecture, Japan. The picture he draws from the nearly 9,000 samples describes the complex interplay between radionuclides released from the Fukushima Daiichi nuclear power plant accident and the marine environment. The chemist showed that the vast majority of fish caught off the northeast coast of Japan remain below limits for seafood consumption, even though the Japanese government tightened those limits in April 2012. Nevertheless, he also finds that the most highly contaminated fish continue to be caught off the coast of Fukushima Prefecture, and that bottom-dwelling fish consistently show the highest level of contamination by a radioactive isotope of cesium. He also pointed out that levels of contamination in almost all classifications of fish are not declining, although not all types of fish are showing the same levels, and some are not showing any appreciable contamination. As a result, he concluded that there may be a continuing source of radionuclides into the ocean, either in the form of low-level leaks from the reactor site itself or contaminated sediment on the seafloor. In addition, the varying levels of contamination across fish types pointed to complex methods of uptake and release by different species, making the task of regulation and of communicating the reasons behind decision-making to the Japanese public all the more

difficult.
Source: http://www.homelandsecuritynewswire.com/dr20121026-understanding-the-effects-of-fukushima-by-studying-fish

3. *October 25, U.S. Nuclear Regulatory Commission* – (Washington) **Columbia nuclear station issued two white findings, severity level III finding.** The Nuclear Regulatory Commission (NRC) determined that two inspection findings at the Columbia Generating Station on the plant's emergency preparedness program are "white," meaning they had low to moderate safety significance, according to a release October 25. The nuclear power plant, operated by Energy Northwest, is located near Richland, Washington. The first white finding involved the licensee's failure to maintain a plan to appropriately characterize emergency action levels which could have delayed recognition of some radiological emergency conditions. The second white finding involved the licensee's failure to maintain adequate methods for assessing and monitoring actual or potential offsite radiation releases from the plant during emergencies. This adversely affected the licensee's ability to assess the consequences of a radiological release and had the potential to impact protective action recommendations necessary to protect public health and safety. These conditions existed between 2000 and 2011 when they were corrected. A violation was also issued because regulations require the licensee to make prompt notification to the NRC of any event that results in a major loss of emergency assessment capability. The NRC identified these issues during its inspection but the licensee did not report them to the NRC in a timely manner, as required. The two white findings will move the Columbia Generating Station into the "degraded cornerstone" column of the NRC's action matrix, resulting in a higher level of NRC scrutiny.
Source: http://www.pennenergy.com/articles/pennenergy/2012/10/columbia-nuclear-station-issued-two-white-findings-severity-level-iii-finding.html

[Return to top]

Critical Manufacturing Sector

See item **25**

[Return to top]

Defense Industrial Base Sector

4. *October 26, Global Security Newswire* – (National) **Nuclear arms oversight difficulties persist, DOE auditors say.** A need to mitigate the expense of efforts to update the U.S. nuclear weapons complex has posed a continuing challenge to the Department of Energy (DOE), its inspector general said in a report issued the week of October 15. Auditors said the department still faces the same difficulties they described in a separate assessment issued November 2011, the Albuquerque Journal reported October 25. Shortcomings in the department's oversight of hired firms continue to raise significant concern, the inspector general stated, noting that related problems extend to protection of DOE assets as well as projects aimed at ensuring the dependability of the

country's atomic arsenal. The report reaffirmed a prior call for the department to eliminate redundant activities within the National Nuclear Security Administration, the semiautonomous DOE branch responsible for overseeing the country's nuclear weapons and related operations. Separately, DOE investigators described security matters as posing "a key management challenge," a move they attributed largely to a high-profile July break-in at the Y-12 National Security Complex in Tennessee. "Given the policy issues that have arisen as a result of this intrusion and the importance of ensuring the safe and secure storage of nuclear materials at department sites, we have elevated safeguards and security to the management challenges list," their report stated.
Source: http://www.nti.org/gsn/article/nuclear-arms-oversight-difficulties-persist-doe-auditors/

5. *October 25, Nextgov* – (National) **Pentagon cyber-threat sharing program lost participants.** A Department of Defense (DOD) effort designed to share information on computer threats with defense contractors lost members, InsideDefense reported. Five of the initial 17 members pulled out of the Defense Industrial Base Enhanced Cybersecurity Services group, a component of the department's cybersecurity information assurance program, a DOD spokesman confirmed. Under the initiative, the government fed threat signatures to Internet service providers that participating defense companies paid to scan their traffic and identify malware, Foreign Policy reported. The program, aimed at offering participants additional security protection, ran in pilot mode for nearly 2 years. "At the end of the operational pilot, one of the commercial service providers withdrew. During the operational testing of the pilot, five of the 17 DIB companies chose to withdraw and reallocate their resources to other corporate priorities," the DOD spokesman told InsideDefense. Four of the five companies that quit during the pilot are considering to rejoin a modified version of the program, Foreign Policy reported. In another arrangement, the companies would cut the ISPs as middlemen, receiving threat signatures straight from the government. DOD apparently is hosting a briefing in coming weeks to inform companies of the initiative, according to InsideDefense.
Source: http://www.nextgov.com/cybersecurity/2012/10/pentagon-cyber-threat-sharing-program-lost-participants/59028/

[Return to top]

Banking and Finance Sector

6. *October 25, Courthouse News Service* – (California; Washington) **Fraud ring guilty of $100 million in fake mortgage applications.** A Los Angeles-based accountant who admitted participating in a fraud scheme by creating fake W-2 forms, pay stubs, and other records for straw buyers so that her fellow conspirators could collect more than $14.5 million in kickbacks from fraudulently obtained mortgage loans pleaded guilty October 25 to wire fraud. In entering her guilty plea, she admitted reviewing payment records that showed the kickbacks were collected from the fraudulent purchase of $100 million in properties. A federal grand jury in September handed up superseding indictments charging a Laguna Hills loan processor for submitting false loan applications using falsified documents to mortgage lenders on behalf of straw buyers in

the same scheme, a U.S. Attorney said. In addition, the loan processor allegedly maintained what he called a "pipeline" of additional properties to purchase as part of the scheme, each of which included an additional $100,000 or more in potential kickbacks. The accountant and loan processor joined other defendants that include an unlicensed mortgage broker, a Ramona real estate agent, the mortgage broker's assistant, and a Seattle businessman. As alleged in court records, the defendants carried out their scheme by recruiting "investors" through the Internet and advertisements in the Los Angeles Times. Each was a straw buyer promised $10,000 for their role in the scheme.
Source: http://www.sandiego6.com/news/local/Wire-Fraud-Ring-Guilty-of-100-Million--175907611.html

7. *October 25, Sunshine State News* – (Florida) **State Attorney: Seven charged in mortgage fraud.** Six individuals from south Florida and one Orlando resident were charged as part of a mortgage fraud scheme that totaled nearly $5 million, according to the Florida Attorney General and Miami-Dade Police Department October 25. According to the release, the scheme operated with straw buyers who used their names and credit to purchase numerous properties. Once the loan had been secured and records reflected a price well over the actual price paid to the seller, a variety of financial exchanges would take place to make the purchase appear legitimate. The laundered money would then go back to the closing agent's escrow account and be characterized in the records as the cash brought to the closing by the straw buyer. Those arrested face charges including grand theft and organized fraud.
Source: http://www.sunshinestatenews.com/blog/state-attorney-seven-charged-mortgage-fraud

8. *October 25, Wall Street Journal* – (International) **Moscow police arrest internet scam suspects.** Russian authorities charged nine West African immigrants with allegedly stealing $28.8 million from hundreds of foreign companies through what police described as an elaborate scheme using bogus passports bearing names that appeared very similar to those of major Russian companies like Gazprom, Rosneft, and Murmansk Shipping Company, the Wall Street Journal reported October 25. The alleged scam targeted firms dealing in minerals, oil and gas, and other commodities operating in the United States, the European Union, China and South-East Asia and had been going on for many years, Russia's interior ministry said in a statement. The alleged fraudsters managed the ruse by using the companies' Russian names on the bogus IDs, which tricked the companies into thinking they were actually doing business with real firms. Raids on the homes of seven of the suspects uncovered counterfeit documents, bogus notary stamps, falsified company paperwork, and printing equipment capable of producing it all, the police said. Investigators said the proceeds of the scam appeared to have been sent to Africa.
Source: http://blogs.wsj.com/emergingeurope/2012/10/25/moscow-police-arrest-internet-scam-suspects/

[Return to top]

Transportation Sector

9. *October 26, Associated Press* – (Florida) **Plane with engine trouble makes emergency landing.** Aviation officials said a Spirit Airlines flight with engine trouble was forced to make an emergency landing at Palm Beach International Airport. A Federal Aviation Administration spokeswoman said Flight 946 was headed to Fort Lauderdale, Florida, from Cartagena, Colombia, when it was diverted October 25. She told the Palm Beach Post that crew members reported the plane had a stuck throttle. A Spirit Airlines spokeswoman said there were 54 passengers and crew on board at the time. The airline provided the passengers with transportation to the Fort Lauderdale airport.
Source: http://www.cbs12.com/template/inews_wire/wires.regional.fl/234bd424-www.cbs12.com.shtml

10. *October 26, Associated Press* – (Georgia) **Several children hurt when school bus, car collide.** Authorities said more than a dozen children were hurt when a school bus and a car collided near downtown Marietta, Georgia. Police said a child passenger in the car was taken by helicopter to a hospital after the October 26 wreck. A Marietta police spokesman told the Atlanta Journal-Constitution that the child's injuries were considered life-threatening. The spokesman said 13 children on the bus were taken to another hospital. Their injuries were described as not life-threatening. He said two students were taken to the hospital by ambulance. The other 11 were taken to the hospital on another bus. A Marietta City Schools spokesman said 37 students were on the bus heading to Marietta High School when the crash occurred.
Source: http://www.wtvm.com/story/19923423/several-children-hurt-when-school-bus-car-collide

11. *October 26, Washington Post* – (Maryland) **Four students, car's driver hurt in Rockville school bus collision.** Four students from Fallsmead Elementary School in Rockville, Maryland, sustained minor injuries when a car hit their school bus head-on October 26, according to authorities. The car's driver was hospitalized with serious injuries, according to a Montgomery County Fire and Rescue Service spokeswoman. The driver was charged with failure to control speed to avoid a collision and crossing the center line of the roadway, said a Rockville Police lieutenant. There were 37 students on the bus, according to a Montgomery schools spokesman. The four with minor injuries "were taken to the hospital as a precaution," he said. The other students were evaluated by a nurse once they reached school and officials called the students' parents. The spokesman said school officials were told the driver of the other vehicle may have passed out before the collision.
Source: http://www.washingtonpost.com/blogs/crime-scene/post/four-students-cars-driver-hurt-in-rockville-school-bus-collision/2012/10/26/75950e06-1f79-11e2-9cd5-b55c38388962_blog.html

12. *October 25, KARE 11 Minneapolis* – (Minnesota) **Students injured after school bus rolls in central Minn.** Six children were treated for injuries after a school bus tipped over in slippery conditions near Little Falls, Minnesota, October 25. Crash reconstruction indicated that the bus, owned by Palmer Bus Company, was traveling

north on Iris Road when the driver lost control on a slippery, sharp curve, causing the bus to tip on its side. Fifteen students, mostly middle and elementary school age, were aboard the bus when it tipped. Four students were initially taken from the scene by ambulance with what were described as minor injuries to be checked out at a hospital in Little Falls. Eventually two more students were also taken by ambulance to be evaluated. Sheriff's investigators said it did not appear the driver was impaired or under the influence of alcohol or drugs.
Source: http://www.kare11.com/news/article/995940/391/Students-injured-after-school-bus-rolls-in-central-Minn

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

13. *October 25, U.S. Food and Drug Administration* – (National; International) **Tropical Valley Foods issues alert on undeclared allergens in dark chocolate, organic dark chocolate, milk chocolate and trail mix products sold in bulk.** October 25, Tropical Valley Foods alerted customers that because of a label error, Dark Chocolate, Organic Dark Chocolate, and Trail Mix items which were sold in bulk quantities contain undeclared allergens. Consumers who have an allergy or severe sensitivity to wheat, soy, or tree nuts run the risk of serious or life-threatening allergic reaction if they consume these products. The products were shipped to distributors and retailers across the United States, as well as Quebec City, Canada; Hong Kong, China; and Dubai, United Arab Emirates. The recall was initiated after a U.S. Food and Drug Administration inspection found that Dark Chocolate, Organic Dark Chocolate, Milk Chocolate, and Trail Mix bulk items had undeclared allergen information on bulk labels. A recall was initiated on the bulk and partial bulk products which were shipped from Tropical Valley Foods during the time frame of September 26, 2011-September 25, 2012.
Source: http://www.fda.gov/Safety/Recalls/ucm325787.htm

For another story, see item **2**

[Return to top]

Water Sector

14. *October 26, Champaign-Urbana News-Gazette* – (Illinois) **Boil order for Tuscola lifted.** A boil order for the city of Tuscola, Illinois, was lifted October 26 following a break in a water main October 25. The city treasurer said the order was necessary because of a break that happened in a new residential development at the corner of

Prairie Street and Northline Road in the northeast part of town. The break was repaired October 25.
Source: http://www.news-gazette.com/news/environment/2012-10-26/boil-order-tuscola.html

15. *October 26, Idaho State Journal* – (Idaho) **Water boil order in effect for large part of Blackfoot.** A water boil order was in effect for a large section of Blackfoot, Idaho, including Blackfoot High School, Stoddard Elementary, and State Hospital South, the Idaho State Journal reported October 26. After a water sample for the area of town east of Fisher Avenue came back positive for coliform bacteria, the boil order was issued by the mayor. "We began mitigating already by flushing water lines and chlorinating," he said. Another sample has been sent in to the Idaho Division of Environmental Quality. If it comes back clean, another sample must be tested to confirm the bacteria threat is over before the boil order can be lifted. "It could be released as soon as Sunday," the mayor said.
Source: http://www.idahostatejournal.com/news/local/article_344926c4-1f08-11e2-95b7-0019bb2963f4.html

16. *October 25, KSL 5 Salt Lake City* – (Utah) **Mercury hits dangerous level in 2 Utah waterways, fish.** State officials October 25 issued an advisory regarding elevated mercury levels found in striped bass in two southern Utah bodies of water. The warning includes fish in Lake Powell from Dangling Rope Marina, south to the dam in Kane and San Juan counties, and Quail Creek Reservoir in Washington County. The advisory also came with revised consumption guidelines. Mercury is a naturally occurring element that can be transformed into methylmercury, a toxic form found in some natural waters. Chronic exposure to low concentrations of methylmercury may result in neurological effects in developing fetuses and children. Previous sampling of mercury had found elevated levels in brown trout at Jordanelle and Porcupine reservoirs, Weber and Duchesne rivers, and the east fork of the Sevier River. Other species of fish in Utah found to have elevated mercury include rainbow trout, wiper, and smallmouth bass. Since 2000, fish in 322 water bodies in Utah have been tested for mercury. Fish with elevated levels of mercury have been found in 21 of the 322 waterbodies.
Source: http://www.ksl.com/?sid=22702497&nid=148

[Return to top]

Public Health and Healthcare Sector

17. *October 26, Associated Press* – (South Carolina) **S.C. has 1st case of fungal meningitis tied to shots.** Health officials reported South Carolina's first probable case of fungal meningitis linked to steroid shots for back pain, the Associated Press reported October 26. An interim State epidemiologist said the South Carolina resident was treated with antifungal medications as recommended by the U.S. Centers for Disease Control and Prevention. The medication made by a specialty pharmacy in Massachusetts has been recalled. The State Department of Health and Environmental Control said additional lab testing is pending confirmation of the diagnosis.

Source: http://www.theitem.com/news/ap_state_news/s-c-has-st-case-of-fungal-meningitis-tied-to/article_7aa725cc-8a2d-5cad-9100-24ccbefe8bb4.html

18. *October 26, WBIW 1340 AM Bedford* – (Indiana) **State fungal meningitis cases up to 43.** Indiana now has 43 cases of fungal meningitis linked to injections of a recalled back pain medication. The Indiana State Department of Health reported two additional cases October 25. The number of deaths remains at three, and Elkhart County's health officer said they were all linked to that county east of South Bend and bordering Michigan. The health department said six Indiana clinics received the tainted steroids, including the OSMC Outpatient Surgery Center in Elkhart. The tainted medication also went to clinics in Columbus, Evansville, Fort Wayne, South Bend, and Terre Haute. Source: http://www.wbiw.com/state/archives/2012/10/state_fungal_meningitis_cases.php

19. *October 26, WJXT 4 Jacksonville* – (Florida) **Macclenny doctor arrested in insurance fraud scheme.** A Macclenny, Florida doctor was arrested on 1 count of organized fraud in a scheme to defraud Medicare, Medicaide, and private insurance of more than $50,000, and 821 counts of false or fraudulent insurance claims. The investigation began late 2011 when investigators identified him as a significant prescriber of controlled substances in northeast Florida, according to the Florida Department of Law Enforcement. Investigators raided his clinic in September 2011 and arrested the office manager and four patients, then shut down the clinic. According to investigators, they discovered evidence that linked him to overprescribing medication to patients as well as allowing unlicensed and untrained staff members to practice medicine. The employees were then directed to inflate medical billing to Medicare, Medicaid, and private insurers for a level of service that the patient did not receive. Interviews with employees indicated that the doctor, a sole practitioner, pushed his untrained medical staff to see 50 or more patients a day and bill for medical issues not addressed and treatment not received, all with the intent of maximizing profit. Source: http://www.news4jax.com/news/Macclenny-doctor-arrested-in-insurance-fraud-scheme/-/475880/17128492/-/32gcau/-/index.html

For another story, see item **15**

[Return to top]

Government Facilities Sector

20. *October 25, WBKO 13 Bowling Green* – (Kentucky) **Monroe County schools receive bomb threat.** Schools across Monroe County, Kentucky, put their safety evacuation plan into action October 25 after Tompkinsville Elementary received a call stating that a bomb had been planted in the school, police said. Shortly after the call, nearly 2,000 students in Monroe County were taken to 3 different safe spots. Kentucky State Police found no evidence of a bomb, and Tompkinsville Elementary was the last school to be cleared. All Monroe County schools were back in session by the end of the day and were cleared of any threat. All after school activities were canceled October 25.

Source: http://www.wbko.com/news/headlines/Monroe-County-Schools-Receive-Bomb-Threat-175875891.html?ref=891

21. *October 25, Fairborn Daily Herald* – (Ohio) **Smoke forces evacuation; school closed.** Students at Warner Middle School in Xenia, Ohio, had classes cancelled October 25 after they were evacuated when smoke was noticed on the second floor. According to fire officials, the fire department was notified that the installation of a new heating and air conditioning system and some roof construction might cause a small amount of smoke. "There was a small fire in the ventilation system that caused more smoke than expected," said the chief of the Xenia Fire Department. Two ladder trucks and four engines responded to the scene. School authorities canceled school for the rest of the day because of excessive smoke on the second floor. Students were moved to the Xenia Community Center, formerly Xenia Nazarene High School. The second floor had heavy smoke, but the nature of other damage was unknown. Classes were canceled for the remainder of October 25, but were expected to be back in session October 26.
Source: http://www.wdtn.com/dpp/news/local/greene_county/smoke-forces-evacuation-school-closed#.UIqo56CBxI0

For more stories, see items **11**, **12**, **15**, and **32**

[Return to top]

Emergency Services Sector

22. *October 25, Associated Press* – (Washington) **WA county jail inmates use ductwork in riot.** The Whatcom County, Washington sheriff said a handful of county jail inmates used metal ductwork ripped from crumbling walls to smash windows and pry off locks in a riot that caused about $10,000 in damage October 24. One inmate was treated for a minor injury. The sheriff said deputies trained in riot response ended the violence at the Bellingham jail after about an hour. The sheriff said six inmates in a maximum security cellblock ripped chunks of the heating system off the walls and used the metal parts as weapons, smashing windows in the interior day room. Toilets were flooded as well. He said the deteriorating condition of the aging jail was a "major contributing factor" to the riot. A corrections chief said the inmates were upset about being in lockdown for a roll call that took longer than usual.
Source: http://seattletimes.com/html/localnews/2019525967_apwawhatcomjailriot.html

23. *October 25, ABC News* – (New York) **'Cannibal' cop plotted to eat 100 women: Feds.** A New York City Police Department (NYPD) officer who allegedly planned to kidnap, cook, and eat as many as 100 women was arrested following a joint NYPD and FBI investigation, ABC News reported October 25. The officer was charged with one count of conspiracy to commit kidnapping, according to a federal criminal complaint, as well was using the National Crime Information Center database to access unauthorized data. The complaint alleged that he exchanged electronic messages with an unnamed co-conspirator "about kidnapping, cooking and eating body parts of [Victim 1]." He allegedly created computer files pertaining to "at least 100 women and

containing at least one photograph of each woman." According to the complaint, he used law enforcement databases to conduct surveillance on potential victims. A U.S. Attorney for the Southern District of New York said the investigation was ongoing.
Source: http://abcnews.go.com/Blotter/cannibal-cop-plotted-eat-100-women-feds/story?id=17562584#.UIquLK7TKCx

24. *October 24, WDRB 41 Louisville* – (Kentucky) **U of L student accused of aiming laser pointer at pilot.** Police surrounded a University of Louisville dorm in Louisville, Kentucky, and arrested a student, saying he could have caused a Louisville Metro Police Department (LMPD) helicopter to crash from his dorm room, WDRB 41 Louisville reported October 24. According to a police report, the student was in his dorm and flashed a laser pointer in the eyes of a LMPD helicopter pilot October 21. School officials said the pilot followed that laser to Unitas Tower and then flashed a light into the student's dorm and called for backup. The student was then arrested by University Police and taken to Metro Corrections. The student was charged with wanton endangerment of a police officer.
Source: http://www.wdrb.com/story/19897114/u-of-l-student-accused-of-hitting-pilot-with-laser-pointer?hpt=ju_bn4

[Return to top]

Information Technology Sector

25. *October 26, Softpedia* – (International) **DoS vulnerability found in wireless chips used by Apple, HTC, Samsung, Ford, others.** Researchers from Core Security's Core Impact team uncovered a remotely exploitable vulnerability in Broadcom BCM4325 and BCM4329 wireless chipsets that could be leveraged by cybercriminals to launch a denial-of-service (DoS) attack. According to advisories published by the U.S. Computer Emergency Readiness Team (US-CERT) and Core Security, the vulnerability is caused by an out-of-bounds read error condition that exists in the chips' firmware. Apparently, an attacker sending an RSN (802.11i) information element can cause the WiFi NIC to stop responding. The flaw affects Apple, HTC, Samsung, Acer, Motorola, LG, Sony Ericson, and Asus products, including iPhone 4, iPod 3G, Xoom, Galaxy Tab, Nexus S, and Evo 4G. The Ford Edge car is also affected. The experts notified Broadcom and although there were some communication problems, the company released an official statement to say a patch was developed. Since many of the affected products are out of service, the patch will be provided to customers on a case-by-case basis.
Source: http://news.softpedia.com/news/DOS-Vulnerability-Found-in-Wireless-Chips-Used-by-Apple-HTC-Samsung-Ford-Others-302384.shtml

26. *October 26, The H* – (International) **Germany gets the most malicious spam.** German email users unseated users from the United States as the recipients of most malicious email messages. According to a report on September's spam by Kaspersky, Germany hit the top of the chart with 13.87 percent of malicious mail being directed at its users, followed by Spain (7.43 percent), Russia (6.85 percent), India (6.39 percent), Vietnam (5.95 percent), Australia (5.94 percent), China (5.80 percent), and the United States

(5.62 percent). The United States led the chart for the previous 8 months. Overall, Kaspersky says 3.4 percent of all emails contained malicious files, a drop of 0.5 percentage points compared to August. Germany saw a six percentage point rise in its detections and Spain saw a four percentage point rise, while United Kingdom's share dropped two percentage points to 4.67 percent. It was also a month for drastic changes in the top 10 malware detected by Kaspersky. Long-term leader "Trojan-Spy.HTML.Fraud.gen" fell out of the top 10 completely, giving its top spot to "Backdoor.Win32.Androm.kv" (aka Backdoor.Trojan and PWS-Zbot.gen.ana), a backdoor trojan which enables remote access, being found in 6.32 percent of the malicious emails. It was followed by "Email-Worm.Win32.Bagle.gt", an email address harvester and malicious program downloader, and then the "Email-Worm.Mydoom.m" and "Mydoom.l" email address harvesters. Also in the top 10 were 4 ransomware trojans.
Source: http://www.h-online.com/security/news/item/Germany-gets-the-most-malicious-spam-1737717.html

27. *October 26, Wired* – (International) **Man claiming half of Facebook arrested on fraud charges.** A man claiming to own half of Facebook was arrested October 25 and charged with a multibillion dollar scheme to defraud the social-networking site and its chief executive and founder. The man, of Wellsville, New York, filed a federal lawsuit in 2010, citing documents and a contract between him and Facebook's CEO that promised him half the company. Facebook made it clear from the beginning that it believed the contract and emails the man produced as evidence were fakes. Facebook told a federal judge that its forensic examiners proved that a 9-year-old contract the man submitted to the court was "forged." The analysis also claimed that 27 emails between Facebook's CEO and the man — some of which mention Facebook — were "fabricated" by the man. Facebook's CEO has said all along that an authentic "Work for Hire" contract between the two involved another project. The man hired Facebook's CEO to work his StreetFax company nearly a decade ago, the CEO claimed. The man, however, alleges the contract also included fronting Facebook's CEO $2,000 in exchange for half of Facebook when he was a college student. Federal authorities agreed with Facebook's CEO and its forensic analysis. The man is accused of one count of mail fraud and one count of wire fraud, authorities said. Each count carries a maximum 20-year term.
Source: http://www.wired.com/threatlevel/2012/10/facebook-fraud-arrest/

28. *October 26, The H* – (International) **Exim mail servers susceptible to DKIM attacks.** There is a critical vulnerability in functions for verifying DomainKeys Identified Mail (DKIM) signatures in the widely used open source mail server Exim. The problem appears to be a buffer overflow on the heap which can be exploited by crafted DNS records to inject code that could compromise the server. According to an announcement on the Exim mailing list (alternative list archive), versions 4.70-4.80 are affected, if DKIM support is included. The developers released version 4.80.1 which specifically fixes this vulnerability. To avoid confusion, the next version will not be named 4.81. As a workaround, DKIM verification can be disabled using the option "warn control = dkim_disable_verify" within an ACL. Both Debian and Ubuntu released packages in which the vulnerability is fixed.

Source: http://www.h-online.com/security/news/item/Exim-mail-servers-susceptible-to-DKIM-attacks-1737670.html

29. *October 25, Softpedia* – (International) **Scam alert: US Customs and Border Protection Service Department package delivery.** Scammers started sending out emails entitled "US Customs and Border Protection Service Department" to trick recipients into thinking they received a package from overseas. "We write to inform you that your package with reference number 2661428 has been in Customs facility custody waiting for resolutions of the clearance to further the delivery to your delivery address by the delivery Agent who came all the way from Africa," the scam emails read. "We have been waiting for you to contact us regarding your consignment box which the agent suppose to deliver to you which was on hold by USA Customs Department and they are requesting for clearance certificate...." The scammers are attempting to convince victims to send back their personal details, including name, contact information, and passport or ID card number.
Source: http://news.softpedia.com/news/Scam-Alert-US-Customs-and-Border-Protection-Service-Department-Package-Delivery-302159.shtml

30. *October 25, ZDNet* – (International) **Google, Yahoo and Microsoft fix email security flaw.** Google, Yahoo, and Microsoft all fixed a vulnerability in their email-signing mechanisms that made it possible for people to spoof messages coming from their systems. The problem was that they were using keys of less than 1,024 bits in length in their implementations of the DomainKeys Identified Mail (DKIM) mechanism. Some consider even 1,024-bit RSA keys as being too easy to crack, but shorter keys are definitely too insecure for serious use currently, as the computational power available in the cloud makes it relatively easy to crack them by brute force. According to a U.S. Computer Emergency Readiness Team (US-CERT) note released October 24, Google, Microsoft, and Yahoo were all using RSA signing keys that were too-short, and all three vendors have now fixed the problem after being notified.
Source: http://www.zdnet.com/google-yahoo-and-microsoft-fix-email-security-flaw-7000006379/

31. *October 25, Ars Technica* – (International) **Backdoor in computer controls opens critical infrastructure to hackers.** Software used to manage equipment in power plants, military environments, and nautical ships contain an undocumented backdoor that could allow malicious hackers to access sensitive systems without authorization. The CoDeSys software tool, which is used in industrial control systems sold by 261 different manufacturers, contains functionality that allows people to remotely issue powerful system commands, a researcher with security firm ioActive, told Ars Technica. The CoDeSys tool will grant a command shell to anyone who knows the proper command syntax and inner workings, leaving systems that are connected to the public Internet open to malicious tampering. Of the two specific programmable logic controllers (PLCs) the researcher tested, both allowed him to issue commands that halted the devices' process control. He estimated there are thousands of other models that also ship with CoDeSys installed, and he said most of them are probably vulnerable to the same types of attacks. He declined to identify the specific models he tested except to say that one ran the Linux operating system on Intel-compatible

processors and the other used Microsoft's Windows CE running on ARM chips. He said a quick search using the Shodan computer location service showed 117 devices directly connected to the Internet, but he suspects more detailed queries could reveal many more. A blog post that contains additional vulnerability details said code that automates the exploit is expected to be added to the Metasploit software framework used by hackers and security professionals.
Source: http://arstechnica.com/security/2012/10/backdoor-in-computer-controls-opens-critical-infrastructure-to-hackers/

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

See item **34**

[Return to top]

Commercial Facilities Sector

32. *October 26, WTVF 5 Nashville* – (Kentucky) **Businesses evacuated after bomb threats in Tompkinsville.** Kentucky State Police searched for the suspect who called in several bomb threats in Monroe County, forcing several evacuations, WTVF 5 Nashville reported October 25. Among the buildings threatened were a school, an office, a store, and restaurants in Tompkinsville. The first call came in October 25 and started a chain reaction that shut down the entire small town. One of the first places to get a threat was Tompkinsville Elementary School. Officials said the students had to be evacuated. Some were sent to a nearby National Guard armory where parents picked them up. All Monroe County schools were shutdown as a precaution. The local Walmart, McDonald's, and Sonic all got the same call — as did the law offices of the Monroe County Attorney. Police went building to building, checking for explosives. None were found, but each location was evacuated as a precaution, forcing people to wait hours until it was deemed safe.
Source: http://www.newschannel5.com/story/19913136/businesses-evacuated-after-bomb-threats-in-tompkinsville

33. *October 26, Chicago Tribune* – (Illinois) **Firefighters battle extra-alarm blaze in Englewood church.** An extra-alarm fire tore through a church in the Englewood neighborhood on the South Side of Chicago October 26. The 3-11 alarm fire broke out at the Love, Faith, and Praise Church of God in Christ. Flames were shooting through the roof when firefighters arrived, according to the Fire Department. Responding crews

surrounded the building and fought the fire from the outside because of concerns the walls or roof might collapse. Nearly 200 firefighters and paramedics responded to the scene, according to a Fire Department spokesman. The cause of the fire was under investigation. Much of the north face of the church was damaged, and two stained glass windows were shattered.
Source: http://www.chicagotribune.com/news/local/breaking/chi-chicago-fire-department-responds-to-extraalarm-blaze-20121026,0,2623884.story

34. *October 25, WFXT 25 Boston* – (Massachusetts) **Explosion, fire knocks power out at Globe.** A manhole explosion and fire caused the Boston Globe in Massachusetts to lose power for a few hours October 24. According to the Globe's Metrodesk Web site, power was knocked out and shut down the paper's newsroom and pressroom for about 3 hours. The paper was able to publish and get out the first edition of the October 25 newspaper, though some readers may have received their paper later than usual.
Source: http://www.myfoxboston.com/story/19910966/fire-knocks-power-out-at-globe

35. *October 25, WWL 4 New Orleans* – (Louisiana) **Electrical issue suspected in Slidell strip mall fire.** Investigators believe electrical problems may have caused a large fire at a Slidell, Louisiana strip mall October 25. Ten businesses in the Corporate Square shopping center were affected by the fire; four from flames and water, the other six from smoke. SuperCuts and We Buy Gold caught the brunt of the damage. Firefighters said the blaze started in the attic space above the SuperCuts and spread across the complex through breaches in the firewalls. An official estimate on the cost of the damage was not complete. There was no word on when any of the businesses would open again.
Source: http://www.wwltv.com/news/Electrical-issue-suspected-in-Slidell-strip-mall-fire-175891951.html

36. *October 25, Reuters* – (Pennsylvania) **Multi-alarm fire heavily damages Lebanon County apartment buildings.** Two families were left homeless in the aftermath of a multi-alarm fire in Lebanon County, Pennsylvania. The fire broke out October 25 in the Palmyra borough. The fire started in an apartment on the second floor of the building and quickly spread to the attic of an adjoining building and then on to a third building. The fire was started by an overturned candle. Damages to the three buildings was estimated at $400,000-$450,000 including contents. About 75 firefighters from 15 fire companies from Lebanon and Dauphin counties battled the fire. There were no reported injuries. The American Red Cross was assisting three adults and two children from two families displaced by the fire with food, clothing, and shelter. A total of 15 people were affected by the fire.
Source: http://www.fox43.com/news/lebanon/wpmt-multialarm-fire-heavily-damages-lebanon-county-apartment-building-20121025,0,378105.story

37. *October 25, City News Service* – (California) **Punctured pipe spills acid next to Corona park.** A ruptured pipe caused muriatic acid to spill poolside at a park in Corona, California, October 25, leading to a hazardous materials cleanup and the temporary closure of a building. The leak was reported around noon adjacent to the pool at the City Park. According to a Corona Fire Department spokeswoman, a pipe

connected to a 700-gallon drum filled with muriatic acid was accidentally punctured by a city employee working at the location. An unknown quantity of the chemical, which is often used in cleaning solutions, collected next to the pool, which was closed at the time, he said, adding that the city employee got a spot of acid on his skin but was not injured. She said two engine crews and the fire department's hazardous materials team — numbering around a dozen personnel — were summoned and immediately contained the minor spill. As a precaution, authorities requested that children in the nearby YMCA "shelter in place" until their parents could retrieve them, the spokeswoman said.
Source: http://www.swrnn.com/2012/10/25/punctured-pipe-spills-acid-next-to-corona-park/

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

38. *October 26, AccessNorthGa.com* – (Georgia) **Corps say Lanier releases to increase.** As drought conditions persist within the Apalachicola-Chattahoochee-Flint (ACF) River basin, the U.S. Army Corps of Engineers (USACE) will increase releases from Lake Sidney Lanier and West Point Lake in Georgia, AccessNorthGa.com reported October 26. "Since May, USACE has been operating under drought operations, allowing the ACF projects to meet system requirements through prolonged drought and to potentially regain storage." the deputy public affairs officer said. USACE has been making minimal releases from Lake Lanier to meet minimum flow requirements at Peachtree Creek near the city of Atlanta. The next two week forecast predicts no rain within the ACF basin. Lake Lanier and West Point must now make greater releases to meet the downstream needs at Lake Seminole and at Walter F. George Lake as it begins to run out of storage. The Flint River has been extremely low since May and is currently experiencing historical low flows, therefore all flows to meet downstream requirements must come from the Chattahoochee.
Source: http://www.accessnorthga.com/detail.php?n=254498

[Return to top]

Department of Homeland Security (DHS)
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/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2273
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@hq.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