Homeland Security

Daily Open Source Infrastructure Report
12 September 2011

Top Stories

- Human error knocked out power to about 5 million customers in California, Arizona, and Mexico, and led to a massive sewage spill that closed several San Diego-area beaches. – *NBC; msnbc.com; Associated Press; Reuters* (See item 1)
- Torrential rains swept over the Washington, D.C. region September 8, triggering flash floods that shut major highways, damaged cars and homes, and forced emergency crews to make scores of water rescues. – *Washington Post* (See item 23)

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. *September 9, NBC; msnbc.com; Associated Press; Reuters* – (California; Arizona; International) **Power restored for many after massive blackout.** San Diego Gas & Electric (SDG&E) restored power to all 1.4 million of its customers who lost electricity in a major blackout. The utility made the announcement September 9, a day after a large swath of the Southwest and parts of Mexico lost electricity, and restoration of power came sooner than expected. The blackout also caused a sewage spill that closed some San Diego-area beaches. All public schools in the city also were closed

September 8 as well as local state universities and community colleges. In Mexico, officials said power was out in northern Baja California's 2 biggest cities, home to roughly 2.5 million people, which are connected to the U.S. power grid. Two reactors at a nuclear power plant along the coast went offline after losing electricity, but officials said there was no danger to the public or workers. Officials blamed "human failure" for the outage, which was apparently linked to the actions of an employee at a substation in Arizona. The source of the trouble was traced to an employee removing a piece of monitoring equipment, officials at Phoenix-based Arizona Public Service Co. said. The ill-fated procedure first caused the failure of a high-power line supplying electricity to Southern California before unleashing a domino effect across the Southwest, officials said. Why that mishap, which normally would have been isolated locally, triggered such a widespread outage was to be a focus of the probe, the officials said. Before midnight, power was restored to some 720,000 users in the region, according to combined tallies provided by officials in Arizona, California, and Mexico. Police stations were forced to use generators to accept emergency calls across the area. There were no signs of widespread looting or other unrest related to the outage. Gas stations were shuttered and most shops and restaurants shut down. A backup system allowed officials to continue operating crossings from Arizona to California, said a Customs and Border Protection spokeswoman.
Source: http://www.msnbc.msn.com/id/44449688/ns/us_news-life/#.Tmoauuwg1kA

2. *September 8, Reuters* – (Mississippi) **BP declares force majeure on Mississippi gas plant.** BP declared force majeure on the Pascagoula natural gas processing plant in Mississippi after it sustained damage from Tropical Storm Lee, the company said September 7. The Destin natural gas pipeline, which is majority owned by BP's Amoco Destin Pipeline Co, feeds into the Pascagoula plant, which has a capacity to process 1.5 billion cubic feet per day of gas. The plant is expected to resume operations September 11, Destin said on its Web site. The company also terminated a force majeure September 7, issued previously for its offshore operations due to the formation of Tropical Storm Lee in the U.S. Gulf of Mexico. Destin was still not able to transport gas from its offshore receipt points to its onshore delivery points, it said in a Web site posting, but it was trying to find alternate delivery points for the gas, "to minimize the impact of the Pascagoula Processing Plant force majeure."
Source: http://af.reuters.com/article/energyOilNews/idAFN1E7870WB20110908

3. *September 8, Associated Press* – (California) **Chevron, California settle on gas tank allegations.** San Ramon-based Chevron and California officials have reached a $24.5 million settlement over allegations that the oil giant violated state laws by failing to properly inspect and maintain underground gas tanks. California's attorney general said since 1998, Chevron U.S.A. Inc. and Chevron Stations Inc. violated anti-pollution laws by tampering with or disabling leak-detection devices. The attorney general said the company also failed to test secondary containment systems, conduct monthly inspections, train employees, and maintain alarm systems at gas stations in 32 counties across California. A judge must still approve the settlement. A hearing is set for September 29 in Alameda County Superior Court.
Source: http://fuelfix.com/blog/2011/09/08/chevroncalifornia-settle-on-gas-tank-allegations/

For more stories, see items **15** and **35**

[Return to top]

Chemical Industry Sector

4. *September 9, Occupational Health & Safety* – (National) **New tool proposed for assessing chemical risks.** The American Chemistry Council September 6 proposed a comprehensive, scientifically based system that could be used by the Environmental Protection Agency (EPA) to decide which chemicals require additional review and assessment, to help the agency update the Toxic Substances Control Act (TSCA). Now 35 years old, the TSCA does not dictate a process to use the information currently available to prioritize chemicals for review, the ACC noted. It said with no system in place, the EPA may be wasting time, energy, and resources gathering and analyzing data on chemicals that are already well understood or are unlikely to pose a significant risk to public health or the environment. The ACC's proposed system would evaluate chemicals against consistent scientific criteria that take into account hazard and exposure, giving each chemical a score based on the criteria and then ranking it based on the scores and EPA's best professional scientific judgment. The rankings would be used to determine which chemicals are referred to EPA's Office of Chemical Safety & Pollution Prevention for further assessment. Before the proposal was announced, ACC representatives met with EPA officials to discuss the tool and how it could inform the agency's stakeholder dialogue on the TSCA update.
Source: http://ohsonline.com/articles/2011/09/09/new-tool-proposed-for-assessing-chemical-risks.aspx?admgarea=news

5. *September 9, India Economic Times* – (International) **Al Qaeda stockpiling chemical weapons.** The ouster of Libyan leader's has provided an opportunity for al Qa'ida and other militant groups to stockpile large amounts of weapons, including chemical and biological weapons, the U.S. President's chief counter-terrorism adviser said recently. "We have indications that individuals of various stripes are looking to Libya and seeing it as an arms bazaar," said the assistant to the President for homeland security and counter-terrorism. "We are concerned about the potential for certain weapons to get into the hands of terrorists," he said. Libya's leader is also known to have accumulated a large stockpile of mustard gas. Recently seized documents suggest that in its final hours, his regime shipped large numbers of gas masks and chemical-protection suits to bases of support, according to the Christian Science Monitor. Human Rights Watch has said there were 20,000 surface-to-air missiles in Libya, and many of those are now missing.
Source: http://economictimes.indiatimes.com/articleshow/9925915.cms

6. *September 8, National Public Radio* – (National) **Hair straightener contains dangerous chemicals, FDA says.** The U.S. Food and Drug Administration (FDA) issued a warning letter to the makers of Brazilian Blowout saying the product contains dangerously high levels of formaldehyde. The National Cancer Institute calls the chemical a cancer-causing substance. The company says the product is safe and that it is working with the FDA to clear up the "misunderstanding." Brazilian Blowout is

marketed as formaldehyde free, but an FDA analysis found unacceptably high levels of methylene glycol, the liquid form of formaldehyde. Levels ranged from 8.7 percent to 10.4 percent, far higher than the 0.2 percent considered safe by the Cosmetic Ingredient Review Panel. The FDA told the California company that makes Brazilian Blowout to stop misleading customers and misbranding its product. The firm's chief executive disagreed, saying the product never exceeded safety levels in Occupational Safety and Health Administration tests. The investigation of Brazilian Blowout was prompted by complaints from an Oregon hair stylist who said she suffered chest and throat pain and nosebleeds after using the product. The FDA said other complaints have included eye irritation, blurred vision, nausea, rashes, and vomiting.
Source: http://www.wbez.org/story/2011-09-08/hair-straightener-contains-dangerous-chemicals-fda-says-91709

7. *September 8, Assoicated Press* – (Missouri) **Chemical maker Hercules to pay $245,521 penalty for leaks at Missouri plant.** A Delaware chemical company will pay $245,521 for violations of the Clean Air Act (CAA) at its plant in the northeast Missouri town of Louisiana. The U.S. Environmental Protection Agency (EPA) said Hercules Inc. violated requirements that it control releases of hazardous air pollutants such as formaldehyde, methanol, and other substances. An EPA inspection in 2007 found the company failed to identify and monitor equipment, and failed to stop visible leaks. The agency said Hercules violated the CAA's Leak Detection and Repair requirements. Louisiana is a Mississippi River town about 80 miles north of St. Louis.
Source:
http://www.therepublic.com/view/story/6d32b78cda3648afb1598e02140d4d5f/MO--Chemical-Plant-Penalty/

For more stories, see items **29**, **40**, and **52**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *September 9, Syracuse Post-Standard* – (New York) **4 fired, 34 disciplined at James A. FitzPatrick Nuclear Power Plant.** A series of investigations by the Nuclear Regulatory Commission (NRC) at the James A. FitzPatrick Nuclear Power Plant in Scriba, New York,has resulted in 4 workers being fired and 34 being disciplined, a spokeswoman for the plant owner said September 8. Meanwhile, federal prosecutors announced that one of the fired workers has pleaded guilty to falsifying tests of emergency respirators. The NRC notified the plant owner that it could face civil actions. No known injuries occurred as a result of the falsified tests. The NRC also found that two unidentified “staff level individuals” acted with ”careless disregard” by not following through on their suspicions that the respirator fit tests were inadequate. Most of the 34 workers who were disciplined were workers who should have known that their “fit tests” for the respirators were either not done or were incomplete.
Source:
http://www.syracuse.com/news/index.ssf/2011/09/4_fired_34_disciplined_at_jame.html

9. *September 9, Nuclear Street* – (Pennsylvania; New York) **Flooding in northeast not expected to shut down nuclear plants.** The remnants of Tropical Storm Lee have caused widespread flooding in Pennsylvania and New York, forcing an estimated 100,000 people from their homes but failing to reach levels that would endanger the states' nuclear plants. All commercial reactors in both states were operating at 100 percent power September 8, according to the Nuclear Regulatory Commission (NRC), with the exception of Peach Bottom 3 in Peach Bottom, Pennsylvania, that operated at 88 percent power in advance of a refueling outage. According to statements from the NRC and utilities, that's likely to remain the case as flood waters reach their peak. At Three Mile Island near Middletown, Pennsylvania, flood waters were expected to crest along the Susquehanna River at 297 feet above sea level September 8, 3 feet below the level that would require an unusual event declaration. Upstream, the plant had also begun abnormal operating procedures for floods, but major safety systems remained well above the water. At Peach Bottom, waters in an adjacent pond were expected to crest at 109 feet. Both units will be shut down if water reaches 111 feet, but the utility was using the Conowingo Dam to control the water levels.
   Source: http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2011/09/09/flooding-in-northeast-not-expected-to-shut-down-nuclear-plants-090901.aspx

10. *September 8, Associated Press* – (Idaho) **Cleanup crews remove final loads of hazardous waste from pit at Idaho National Laboratory.** Cleanup crews at Idaho National Laboratory near Idaho Falls, Idaho, have removed the final few loads of radioactive and hazardous waste from one of the most notorious waste pits at the site. Technicians wrapped up work the week of August 29 on Pit 9 from the Radioactive Waste Management Complex located at the eastern Idaho research lab. During the 1960's, thousands of barrels and boxes of radioactive and hazardous waste was dumped into the pit, then covered over with soil. The Idaho Falls Post Register reported the achievement marks the end of a process that started in the 1990s.
    Source: http://www.therepublic.com/view/story/6c9deda0a54e473688beeffd33c797a0/ID--INL-Pit-Cleanup/

11. *September 8, Los Angeles Times* – (California) **Blackout shuts down San Onofre nuclear reactors.** The blackout affecting large swaths of San Diego County in California led to a shutdown of two reactors at the San Onofre nuclear power plant September 9. A spokesman for Southern California Edison said the power outage did not cause any safety issues. A fluctuation in power caused the reactors to shut down at 3:38 p.m., but the the overall plant continues to have power. The spokesman said the system worked as it was supposed to during a loss of power.
    Source: http://latimesblogs.latimes.com/lanow/2011/09/blackout-san-onofre-reactor.html

For more stories, see items **1** and **14**

[Return to top]

Critical Manufacturing Sector

12. *September 7, Associated Press* – (Arkansas) **Worker dies in accident at Magnolia steel mill.** A worker at a steel mill owned by CMC Steel Arkansas in Magnolia died September 6 after an accident that occurred while changing a cable on an overhead crane, the Magnolia Banner-News reported. The coroner said the man was the leader of a maintenance crew that was changing the cable. The U.S. Occupational Safety and Health Administration confirmed September 7 it was investigating. CMC Steel's director of operations said the company was working with local and federal authorities to determine the cause of the accident.
Source: http://www.canadianbusiness.com/article/43704--worker-dies-in-accident-at-magnolia-steel-mill

[Return to top]

Defense Industrial Base Sector

13. *September 8, Bloomberg* – (National) **Sikorsky charges U.S. Army $2,393 for $181 Black Hawk part.** Bloomberg reported September 8 Sikorsky Aircraft Corp. overcharged the U.S. Army for 28 UH-60 Black Hawk helicopter spare parts, including $2,393.41 for a plastic wiring box cover worth $181.70, according to the office of the Defense Department's Inspector General. Sikorsky, a unit of Connecticut-based United Technologies Corp., charged the Army $7,814.88 for a rotor used to cool radiator oil that cost another Pentagon agency $1,536.65, the audit found. Itt cited excessively priced parts and costs based on pricing data that was not current, complete, or accurate from the latest of three Sikorsky contracts with the Corpus Christi, Texas, Army depot. The contracts were valued cumulatively at about $1.1 billion. The initial award was made in December 2002. Army officials have a "myriad of issues to overcome to ensure that prices are fair and reasonable," said the audit. Overall "we calculated that Sikorsky charged the Army $11.8 million, or 51.4 percent more than fair and reasonable prices," between 2008 and 2010, the audit said. About $158,531 of that excess was paid for the plastic wiring box covers.
Source: http://www.bloomberg.com/news/2011-09-08/sikorsky-charged-army-2-393-for-181-black-hawk-plastic-part-audit-finds.html

14. *September 8, ComputerWorld* – (National) **RSA spearphish attack may have hit U.S. defense organizations.** Computerworld reported September 8 that the hackers who broke into EMC's RSA Security division last March used the same attack code to try to break into several other companies, including two U.S. national security organizations, according to data provided by the VirusTotal Web site. Before the attack was publicly disclosed in mid-March, the same maliciously encoded Excel spreadsheet involved in the RSA Security attack had been uploaded to the VirusTotal service's battery of antivirus checks 16 times from 15 different sources. The malware was detected by none of the site's 42 antivirus engines. The code was embedded in Excel documents, but the flaw it exploited when the documents were opened lay in Adobe's Flash Player. According to VirusTotal's founder, two of the targets were entities related to U.S.

national security. The Contagio Malware Dump blog listed four different Excel files used in attacks, including a Nuclear Radiation Exposure And Vulnerability Matrix(dot)xls file that was doctored to look as though it came from the U.S. Nuclear Regulatory Commission. It's not clear who this file was sent to, but in the March 17 spearphishing e-mail also published on the blog, the attackers seemed to target people interested in the recent Japan earthquake. With the subject line, "Japan Nuclear Radiation Leakage and Vulnerability Analysis," the e-mail states, simply, "The team has poured in heart and full dedication into this. Would be grateful if you appreciate it."
Source: http://www.computerworld.com/s/article/9219873/RSA_spearphish_attack_may_have_hit_U.S._defense_organizations?taxonomyId=13

15. *September 7, ABC News* – (International) **Former NASA, DOD scientist pleads guilty to attempted spying for Israel.** A former government scientist who ran many highly classified projects for NASA, the Defense Department, and the Department of Energy pleaded guilty September 7 to attempted espionage for his efforts to sell classified information to Israel. The man, from Chevy Chase, Maryland, was arrested October 19, 2009, in Washington, D.C. by the FBI after he believed he was meeting with Israeli intelligence agents to pass information to them in exchange for money. The FBI began its investigation in 2002 when agents executed a search warrant at his home in a fraud investigation and discovered classified documents. The man, who established his own company, ACT, had been under criminal investigation by NASA's Office of the Inspector General for submitting false billing records to NASA and the Defense Department as part of his contracting work. According to court records, in January 2009, as he traveled overseas, a security check of his personal bags indicated he had two computer thumb drives. However, when he returned on his trip, the drives were no longer in his possession, according to the government. The FBI used an undercover agent to approach the man in September 2009, who told the man he worked for Israeli intelligence. During a lunch meeting with the agent, the man indicated he was willing to work for Israeli intelligence and provide them data. In the next several months, the FBI lured him into using "dead drops," where the man left envelopes with encrypted thumb drives with top secret information about key U.S. weapon and satellite systems in exchange for cash.
Source: http://abcnews.go.com/blogs/headlines/2011/09/former-nasa-dod-scientist-pleads-guilty-to-attempted-spying-for-israel/

For another story, see item **49**

[Return to top]

Banking and Finance Sector

16. *September 9, Federal Bureau of Investigation* – (National) **Marlborough man admits role in multi-million-dollar bank fraud conspiracy.** The U.S. Attorney for the District of Connecticut announced that a 48-year-old man pled guilty September 9 to one count of conspiracy to commit bank fraud stemming from his involvement in a multi-million dollar scheme. According to court documents, the man worked for

Branford-based New England Cash Dispensing Systems, Inc. (NECDS). Beginning in March 2000, NECDS entered into an agreement with Domestic Bank of Cranston, Rhode Island, whereby NECDS would supply ATM services. The ATMs in the network were stand-alone machines in commercial establishments and other locations throughout several northeastern states. In pleading guilty, the man admitted he and others engaged in a conspiracy to defraud Domestic of cash the bank supplied for use in the ATMs. As part of the scheme, he and other NECDS personnel ordered excess cash from Domestic and then diverted the cash, which was meant to be used to refill Domestic ATMs, to refill ATMs that would otherwise have been refilled with NECDS's funds. He and others also engaged in a "cover-up" to prevent the bank from recognizing that money was missing by "floating" Domestic's money. This was done regularly over several years, and resulted in Domestic receiving false data through the periodic replenishment process. Domestic ultimately lost about $4.8 million in funds it had supplied to NECDS. In pleading guilty, the convict admitted he personally stole about $2 million in cash, which he used for his own personal enrichment.
Source: http://7thspace.com/headlines/393534/marlborough_man_admits_role_in_multi_million_dollar_bank_fraud_conspiracy.html

17. *September 9, Phoenix Business Journal* – (Arizona) **Former bank execs settle FDIC lawsuit for $20 million each.** The ex-chief executive of First National Bank (FNB) of Arizona and a former director settled a lawsuit brought by the Federal Deposit Insurance Corporation (FDIC) August 23, alleging the two "sacrificed safety" and promoted risky loans that ultimately caused the bank's failure. The pair agreed to settle for $20 million each, while denying all allegations in the complaint As part of the settlement, the FDIC agreed not to collect the judgments against them if the pair waived their right to sue Lloyds of London Catlin Syndicate, which insured both men. The broader settlement agreement, which is not public, also included other former officers and directors of FNB. In its original complaint, the government agency sought to recover more than $193 million in damages resulting from the directors' and officers' breaches of fiduciary duties, including "gross negligence." In its complaint, the FDIC alleged FNB created a wholesale mortgage division to purchase and market billions of dollars in risky nontraditional mortgages dubbed "Alt-A" loans. The loans boosted FNB's profits to record levels in the short-term, but eventually caused the bank's failure when the real estate market softened. The pair promoted the risky mortgages "long after they should have known the loans being made created a substantial harm to the bank," FDIC documents said.
Source: http://www.bizjournals.com/phoenix/print-edition/2011/09/09/former-bank-execs-settle-fdic-lawsuit.html?page=all

18. *September 9, U.S. Securities and Exchange Commission* – (Texas) **SEC charges solicitor in investment scheme targeting deaf community.** The Securities and Exchange Commission September 8 charged a Corinth, Texas man with securities fraud for soliciting more than $3.45 million from several thousand deaf investors in an investment scheme that the SEC halted last year. The SEC previously charged Imperia Invest IBC with securities fraud and obtained an emergency court order to freeze the investment company's assets. In the complaint, the SEC alleges that the man, who is

deaf, solicited investments for Imperia over a 3-year period from others in the deaf community, promising them he would invest in Imperia on their behalf. What he did not tell investors is that he was misappropriating a portion of their funds to pay his mortgage, car payments, car insurance, and a variety of other personal expenses. He sent the remaining amounts to Imperia's offshore bank accounts. While Imperia guaranteed returns of 1.2 percent per day on these investments, investors have never been paid any interest after giving their money to the man to invest. Even after the SEC charged Imperia and issued an investor alert about the scheme, he continued to reassure investors that Imperia was legitimate and they would be paid. According to the SEC's complaint, the man's investors transferred funds to him via money orders that he then cashed and deposited into accounts he controlled. From there, he forwarded funds to Imperia. He initially sent money to Paypal-like accounts in Costa Rica, Panama, and the British Virgin Islands, but later wired it directly to bank accounts with no apparent link to Imperia in such various other countries as Cyprus and New Zealand.
Source: http://www.sec.gov/news/press/2011/2011-181.htm

19. *September 8, CNN* – (International) **U.S. sanctions Venezuelan officials for allegedly helping FARC rebels.** The U.S. Treasury Department September 8 added four Venezuelan officials to its drug "kingpin" list for allegedly providing arms and security to the Revolutionary Armed Forces of Colombia (FARC) leftist guerrilla group. A loyalist of the Venezuelan president and three other officials are now on the list, the Treasury Department said. The others receiving the designation of "Specially Designated National" under the Foreign Narcotics Kingpin Designation Act are the alternate president of the Latin American Parliament; a major general in the Venezuelan army; and an officer in the country's intelligence service. Their assets are now blocked, and U.S. citizens are generally prohibited from dealing with them. The U.S. government designated the FARC as a "significant foreign narcotics trafficker" in 2003. Treasury's statement alleged one of the men "has facilitated arms sales between the Venezuelan government and the FARC"; another "has used his position to establish an arms-for-drugs route with the FARC"; a third "has served as a primary arms dealer for the FARC, and is a main conduit for FARC leaders based in Venezuela"; and the fourth "has coordinated security for the FARC".
Source: http://edition.cnn.com/2011/WORLD/americas/09/08/venezuela.ofac.list/

20. *September 8, Softpedia* – (National) **Financial services company impersonated in malware spreading campaign.** The Automated Clearing House (ACH), a financial service offered by the U.S. electronic payments association National Automated Clearing House Association (NACHA), was impersonated in a campaign of spam messages sent out to unsuspecting users with the purpose of spreading malware. The samples investigated by MalwareCity seemed to be sent from a legitimate NACHA e-mail account. This specific message, named "ACH Transfer Review," informs the victim a transaction has failed and that she must review the input data for the payment. She then must fill the application form attached to the e-mail. The attachment is represented by a zip file that contains what seems to be a .pdf document that must be reviewed by the recipient. The .pdf file is actually an executable that installs a downloader on the soon-to-be infected computer. The downloader's purpose is to get other malware from the Web, and onto the computer. A few moments later, the Zeus

bot, also known as Trojan(dot)Generic.6152125, is installed on the machine, closely monitoring all electronic financial transactions and sending out username and password information. The routing details from the message appear to come from a domain called ”digitalskys.com”, the Web site of a wireless solutions company, likely used by the cybercriminals to mask their true identity.
Source: http://news.softpedia.com/news/Financial-Services-Company-Impersonated-in-Malware-Spreading-Campaign-220765.shtml

21. *September 8, U.S. Department of Justice* – (Arizona) **Four Tucsonans indicted for mortgage fraud conspiracy.** A federal grand jury in Arizona returned an indictment September 8 charging four defendants in a mortgage fraud conspiracy. The indictment charged 20 counts, including conspiracy to commit bank fraud, false statement to influence a financial institution, and conspiracy to commit transactional money laundering. “The indictment alleges that the defendants fraudulently obtained loans for 19 properties that eventually ended in foreclosure,” said the acting U.S. attorney. It alleges the defendants conspired to commit mortgage fraud to obtain 19 loans totaling about $5.85 million in 2006 and 2007. According to the indictment, two of the defendants purchased properties using various business entities with which they were associated. Thereafter, they sold these properties to straw buyers for a profit. The indictment further alleges the defendants submitted loan applications and other documents that contained material false representations relating to the purchase of the 19 properties. After the fraudulently obtained loan proceeds were received, portions were diverted into the suspects' bank accounts. As a result of the scheme, each of the properties referenced in the indictment went into foreclosure.
Source: http://tucsoncitizen.com/view-from-baja-arizona/2011/09/08/four-tucsonans-indicted-for-mortgage-fraud-conspiracy/

22. *September 8, U.S. Securities and Exchange Commission* – (Massachusetts) **Commission sues Massachusetts investment adviser for fraudulently inducing clients to invest in forex, causing investor losses of nearly $4 million while adviser earned hefty fees.** The U.S. Securities and Exchange Commission (SEC) announced September 8 it filed a civil injunctive action in federal district court in Massachusetts against registered investment adviser EagleEye Asset Management, LLC, and its sole principal in connection with their fraudulent conduct toward advisory clients. In its complaint, the SEC alleges that, between at least April 2008 and August 2010, the head of EagleEye made material misrepresentations to a dozen or so advisory clients to induce them to liquidate investments in securities and instead invest the proceeds in foreign currency exchange (forex) trading. These investments, which were not suitable for older clients with conservative investment goals, resulted in steep losses for clients, totaling nearly $4 million, but EagleEye and its head came away with more than $300,000 in performance fees on the investments, in addition to other management fees. His strategy was to generate temporary profits on forex investments to enable him to collect performance fees, after which client investments invariably would sharply decline in value. According to the SEC's complaint, the man's material misrepresentations to clients concerned the nature of forex investments, the risks involved, and his expertise and track record. The complaint further alleges that, in the case of two clients, without their knowledge or consent, the suspect liquidated

securities in their brokerage accounts and transferred the proceeds to their forex accounts where he lost nearly all client funds, but not before first collecting performance fees for EagleEye (and ultimately himself) on short-lived profits. The complaint said he accomplished the unauthorized transfers by doctoring asset transfer forms.
Source: http://www.sec.gov/litigation/litreleases/2011/lr22086.htm

For more stories, see items **46** and **49**

[Return to top]

Transportation Sector

23. *September 9, Washington Post* – (Maryland; District of Columbia; Virginia) **Torrential rains inundate D.C. region: 3 killed, roads and schools closed.** Torrential rains swept over the Washington, D.C. region September 8, triggering flash floods that killed two people in Fairfax County, Virginia, and one in Anne Arundel, Maryland. Rising waters trapped scores of terrified motorists, forced hundreds to evacuate their homes, and shut major highways, including Interstate 66, and the Capital Beltway. The victims included a 12-year-old boy who was swept away by the flood-swollen waters of Piney Branch Creek in Vienna, Virginia; a 60-year-old man in Great Falls, Virginia who was killed near his stranded vehicle; and a 49-year-old man who drowned in Pasadena, Maryland, authorities said. The Virginia Department of Transportation (VDOT) and state police ordered the Beltway closed from Route 1 to the Mixing Bowl at Interstate 395, as the waters of Cameron Run spilled onto the highway, a VDOT spokeswoman said. Maryland officials closed the Woodrow Wilson Bridge to keep cars off the flooded portion of the Beltway in Virginia. Interstate 66 was also closed westbound near Route 50. The unrelenting rains, sometimes falling at 4 inches an hour, closed schools, courthouses, and government buildings in Prince George's and Charles counties, Maryland. Cars were flooded at a park-and-ride lot in Reston, Virginia, and at auto dealerships in Upper Marlboro, Maryland. Commuter trains were halted. Basements flooded. People were stranded. Homes were evacuated in Prince William, Prince George's, and Fairfax, Virginia. Fairfax and Prince William County officials decided to close schools September 9 because so many roads were flooded, and Prince William declared a local state of emergency. Virginia Railway Express closed its two train lines September 9 because of flooded tracks. Fairfax fire and rescue teams rescued more than 100 stranded motorists, including 12 on Cinderbed Road in Lorton, Virginia. Six were helped from their cars on Interstate 95 at Telegraph Road, a county spokesman said. Earlier in the day, rescue workers in Prince George's helped scores of similarly stranded drivers. County officials said they were keeping an eye on 19 state-regulated dams, most of them in the Pohick watershed.
Source: http://www.washingtonpost.com/local/tropical-storm-lee-inundates-dc-region/2011/09/08/gIQA7OHIDK_story.html?hpid=z2

24. *September 9, Centre Daily Times* – (Pennsylvania) **I-80, Turnpike reopen after floodwaters recede.** Interstate 80 in Columbia County, Pennsylvania and a 39-mile section of the Pennsylvania Turnpike between the Harrisburg and Reading

interchanges, both closed September 8 by flooding, have reopened. According to the Pennsylvania Department of Transportation (PennDOT), I-80 between the Buckhorn Exit 232 and Lightstreet Exit 236, were assessed by PennDOT inspectors for flood-related damage. None was found. The interstate was closed around mile marker 234 when floodwaters overtopped the highway about 4:30 a.m. September 8. The section of turnpike was closed September 8 because officials said flooding from Tropical Storm Lee jeopardized the safety of a bridge over Swatara Creek in hard-hit Dauphin County. Officials said the water level dropped enough overnight to allow engineers to check the bridge's structural integrity and confirm it is safe to carry traffic.
Source: http://www.centredaily.com/2011/09/09/2906716/i-80-turnpike-reopen-after-floodwaters.html

25. *September 9, International Business Times* – (New York; District of Columbia; National) **Amid credible terror threat, NYC Mayor Bloomberg rides Subway, urges residents to 'go back to work'.** Amid a credible terrorist attack threat against New York and Washington, D.C. around the upcoming 10th anniversary of the September 11th attacks, the New York mayor rode the subway September 9 in the effort to assure the city's 8 million residents that preparations are in place. U.S. officials said September 8 they were chasing down a credible but unconfirmed al-Qa 'ida threat to use a car bomb on bridges or perhaps tunnels in New York or Washington — both areas that were attacked almost a decade ago on September 11, 2001. New York police have said in light of the credible threat they are beefing up security at bridges and tunnels, and setting up vehicle checkpoints. Police are implementing bomb sweeps of parking garages and towing more illegally-parked cars, they said. New York commuters have been told they will see a show of force at major transportation terminals, including Grand Central, Penn Station, and near the Port Authority and Times Square subway station. Law enforcement officials are pursuing three individuals who may be traveling to the United States or have perhaps recently entered the country, based on the information received by intelligence officials, authorities said.
Source: http://www.ibtimes.com/articles/211321/20110909/al-qaida-terror-threat-new-york-washington-bloomberg-subway.htm

26. *September 9, Associated Press* – (New York; National; International) **Lee causes more Amtrak disruptions in upstate NY.** Amtrak said flooding in upstate New York is causing more cancellations west of Albany. Amtrak said Empire Service trains will operate normally only between New York City and the Albany-area station in Rensselaer September 9 while repairs are made. Runs of the westbound Lake Shore Limited from New York and Boston to Chicago via Rensselaer also were canceled. Operating normally west of Albany September 9 will be the Maple Leaf, which will be subject to delays between Toronto and Buffalo. Also scheduled to operate normally are September 9's eastbound Lake Shore Limited from Chicago, the Adirondack between Montreal and New York, and the Ethan Allen Express to Rutland, Vermont. ross-state Amtrak passenger service was canceled September 8 because of extensive flooding near Amsterdam, where the tracks run along the north bank of the Mohawk River.
Source: http://online.wsj.com/article/AP5017bd63415344c3af2c51bc279182bd.html

For more stories, see items **2**, **28**, **29**, **44**, **57**, and **58**

[Return to top]

Postal and Shipping Sector

27. *September 9, Associated Press* – (Oregon) **Man, 73, crashes pickup into OR post office.** Oregon State Police (OSP) said a 73-year-old man crashed his pickup truck into the post office in the small central Oregon town of Gilchrist. An OSP lieutenant said the man was driving to get his mail September 8 when he hit the building, damaging the front exterior and interior walls. There were no injuries reported.
Source: http://www.chron.com/news/article/Man-73-crashes-pickup-into-OR-post-office-2162180.php

[Return to top]

Agriculture and Food Sector

28. *September 9, Associated Press* – (National) **Sheriffs: Tall corn creates hazard on rural roads.** Tall stalks obstructing drivers' views are a fall hazard in the Corn Belt, but the danger could be greater as farmers seek to cash in on higher prices by expanding their fields closer to the edge of roads. With corn commanding twice what it did in 2011, farmers from Pennsylvania to the Dakotas have tried to plant as much as possible. The federal government has estimated planting at 92.2 million acres, up 5 percent from in 2010. In some cases, farmers have planted right up to the gravel in remote areas, a practice that can have deadly consequences at unmarked intersections. A Nebraska man was killed the week of August 29 when a pickup truck struck the four-wheeler he was driving on a road near his home. Officials in Iowa, the top corn-growing state, said they were concerned about visibility. Twenty-eight people have died since 2001 at rural intersections where vision was obstructed, according to the Iowa Department of Transportation (IDOT). The department's data does not differentiate between tall corn and other vegetation, but an IDOT spokesman said the crashes tend to occur in the late summer and early fall when corn is high.
Source: http://news.yahoo.com/sheriffs-tall-corn-creates-hazard-rural-roads-070303962.html

29. *September 9, Denver Post* – (Colorado) **Dropped keg sparks flash fire in Downtown Denver brew pub, knotting traffic; no injuries.** A chemical spill and flash fire at a Denver brew pub September 9 forced the evacuation of the building and knotted up traffic. The fire started about 7:15 a.m. at the Rock Bottom Restaurant and Brewery, a Denver Fire Department spokesman said. The fire was quickly put out, and there were no injuries. The fire department's hazmat team was on the scene monitoring the situation as a safety precaution. There was a spill of chlorine dioxide at the brew pub September 6, the spokesman said. It was mopped up and the spill did not cause a problem until September 9, when a worker dropped a keg. A spark from the metallic keg ignited remnant residue of the spill and fueled a flash fire. Police and firefighters shut down Curtis Street from 15th to 17th Street as the fire and chemical residue was

being mopped up.
Source: http://www.denverpost.com/breakingnews/ci_18859710

30. *September 9, Food Safety News* – (New York; New Jersey; Connecticut) **Allergy alert: Raisins recalled for sulfites.** Best Food Cash & Carry Inc. of Maspeth, New York recalled 14-ounce packages of "Deer Raisin Golden" raisins because they contain undeclared sulfites. Consumers who have severe sensitivity to sulfites run the risk of serious or life-threatening allergic reactions. The problem was discovered after routine sampling by the New York State Department of Agriculture and Markets Food Inspector, and subsequent analysis by Food Laboratory personnel, the company said in a news release. The consumption of as little as 10 milligrams of sulfite per serving has been reported to elicit severe reactions in some asthmatics, including anaphylactic shock in some sensitive individuals. Analysis revealed the raisins contained 11.07 milligrams per serving. The presence of sulfites was not declared on any label. No illnesses have been reported to date. The recalled raisins were distributed in 14-ounce, clear, uncoded, plastic packages in New York, New Jersey, and Connecticut retail stores.
Source: http://www.foodsafetynews.com/2011/09/allergy-alert-raisins-recalled-for-sulfites/

31. *September 8, CNN* – (Georgia) **Georgia police: Woman dies after exposure to odor at McDonald's.** An 80-year-old Ponte Vedra, Florida woman died, and at least eight other people were hospitalized after being exposed to an odor at a McDonald's restaurant in Pooler, Georgia, a police chief said September 8. Police and fire personnel were called to the eatery at about 11:50 a.m. September 7, the Pooler police chief said. He said upon arrival, first responders found two people unconscious in the women's restroom and also "became stricken (by) an odor." The Pooler fire chief said crews "immediately backed out and put on their breathing apparatus," at which point they re-entered the bathroom. Authorities were able to bring the women outside and begin providing medical attention, including CPR. Nine people, including three firefighters, were transported to a local hospital. The police chief said that although an investigation is under way, authorities do not anticipate filing criminal charges.
Source:
http://edition.cnn.com/2011/US/09/08/georgia.mcdonalds.death/index.html?hpt=hp_t2

32. *September 8, Hermiston East Oregonian* – (Oregon; Washington) **Harmful potato disease appears in Eastern Oregon.** Researchers in Oregon have discovered for the first time in Umatilla and Morrow counties a potentially devastating disease affecting potato crops. Plant pathologists confirmed September 2 the presence of zebra chip in five different potato varieties in the southern Columbia Basin. The affected varieties are Russet Ranger, Umatilla Russet, Pike, Alturas, and Russet Norkotah, which account for most of the acreage in the basin, said a U.S. Department of Agriculture plant pathologist.
Source: http://www.eastoregonian.com/news/agriculture/harmful-potato-disease-appears-in-eastern-oregon/article_58edb72c-da3c-11e0-87bd-001cc4c03286.html

[Return to top]

Water Sector

33. *September 9, Associated Press* – (National) **Sewage-tainted floodwaters threaten public health.** Floodwaters from the remnants of storms Lee and Irene — tainted with sewage and other toxins — threaten public health in parts of the Northeast by direct exposure or the contamination of private water wells, officials said September 9. A dozen Vermont towns flooded by Irene were still on boil-water orders 12 days later, though officials reported no water-borne illness. Similar precautions have been taken throughout other storm-damaged states. In Waterbury, Connecticut, the municipal wastewater plant was overwhelmed by flooding from Irene, and raw sewage flowed into the Winooski River. On September 7, the Vermont Agency of Natural Resources said septic tanks continued to be a threat since the storm hit August 28. New York City officials said any threat from Irene's backwash had passed, but upstate, 23 municipal water systems had boil-water orders for varying lengths of time. As some communities in New Jersey and Pennsylvania were taking similar precautions after Irene, the unrelenting rains of Lee were expected to trigger more. Officials in Maryland, Delaware, and the District of Columbia, which were also hit hard by Irene, said drinking-water quality had not been compromised. In addition to concerns about water-borne illness, residents of affected areas were being urged to avoid exposure to water and mud possibly polluted with household chemicals and paints.
    Source: http://www.ajc.com/news/nation-world/sewage-tainted-floodwaters-threaten-1164721.html

34. *September 9, Mechanicsburg Patriot-News* – (Pennsylvania) **Boil water advisory in place for Dauphin and Perry counties.** Rising water that inundated a United Water Pennsylvania treatment plant spurred the company to issue a boil advisory for all customers in Dauphin and Perry counties, the Mechanicsburg Patriot-News reported September 9. Included in the warning were the boroughs of Dauphin, Highspire, Hummelstown, Marysville, Paxtang, and Penbrook, and the townships of Lower Paxton, Middle Paxton, Susquehanna, Lower Swatara, Rye, Swatara, and South Hanover. Pennsylvania American customers in parts of Dauphin and Lebanon counties near the Swatara Creek were asked to conserve water because flooding was affecting the Hershey pumping center. In Harrisburg, utilities were being shut off to the Shipoke riverfront neighborhood as well as low-lying sections of midtown from Front Street to Green Street, and from Reily Street north to Vaughn Street.
    Source:
    http://www.pennlive.com/midstate/index.ssf/2011/09/boil_water_advisory_in_place_f.html

35. *September 9, San Diego Reader* – (California) **Sewage spills close area beaches.** Two sewage spills caused by power outages September 8 caused health officials to close a number of beaches near San Diego, California. All beaches north of Scripps Pier through Del Mar and Solana Beach were deemed unsafe after 3.2 million gallons of sewage spilled from the San Diego Metropolitan Wastewater System's Pump Station 64 into the Los Penasquitos Lagoon. A smaller spill at another pump station near I-5 and SR-54 dumped 120,000 gallons into the Sweetwater River, which flows into San Diego Bay.

Source: http://www.sandiegoreader.com/weblogs/news-ticker/2011/sep/09/sewage-spills-close-area-beaches/

For more stories, see items **1**, **40**, and **57**

[Return to top]

Public Health and Healthcare Sector

36. *September 9, San Francisco Chronicle* – (California) **Stanford Hospital ER data put on website for year.** Confidential medical data that includes patient names and diagnoses for 20,000 people seen in Stanford Hospital's emergency room in Palo Alto, California, was posted on a public Web site for nearly a year before hospital officials found out about the security breach. Hospital officials said September 8 that the information has been removed and that they are investigating the incident. They learned of the breach in August. Stanford had sent names, diagnosis codes, account numbers, admission dates, and charges to an outside vendor, Multi Specialties Collection Services in Los Angeles, which handles billing for the hospital, said a hospital spokesman. The patients were all seen between March 1 and August 31, 2009. The billing vendor passed the information on to a subcontractor, which created a spreadsheet out of the data. That spreadsheet was then posted September 9, 2010 to a Web site called Student of Fortune, in a section where students pay for homework assistance. The spreadsheet was uploaded as an attachment to a question about making bar graphs. The spreadsheet remained on the Web site until August 22, when a patient found it and reported it to Stanford. The spreadsheet was removed within 24 hours, and patients were notified of the security breach a few days later. The posted spreadsheet did not include Social Security numbers, birth dates, or any other data that could be used for identity theft, but the hospital is offering free identity protection services to those whose information was made public.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/09/08/BA1Q1L23AP.DTL

37. *September 7, WCNC 36 Charlotte* – (North Carolina) **Charlotte doctor fined for dumping patients' information.** North Carolina's attorney general announced September 7 that a doctor of the Carolina Center for Development and Rehabilitation in Charlotte has paid $40,000 for illegally dumping 1,000 files containing patients' financial and medical information at the West Mecklenburg Recycling Center in June 2010. The files contained names, addresses, dates of birth, Social Security numbers, drivers' license numbers, insurance account numbers, and health information for 1,600 people. The records disposed of by Carolina Center were recovered by Mecklenburg County officials, who contacted the attorney general's office. Under a state law, businesses that dispose of records that contain personal identifying information are required to destroy or shred those records.
Source: http://www.wcnc.com/news/local/Charlotte-doctor-fined-for-dumping-patients-infomation--129387253.html

For another story, see item **43**

[Return to top]

Government Facilities Sector

38. *September 9, Associated Press* – (Nevada) **8 military personnel injured in shelter collapse.** Officials said eight military personnel received minor injuries when a set of aircraft shelters collapsed during a severe wind storm at Nellis Air Force Base near Las Vegas. Base officials said the injured personnel were transported to the hospital after the September 8 evening wind storm. The Nellis spokesman said a majority of the injured had been released late September 8. Officials said they are still assessing the damage done to aircraft and other resources.
Source: http://www.mysanantonio.com/news/article/8-military-personnel-injured-in-shelter-collapse-2162271.php

39. *September 8, KFDM 6 Beaumont* – (Texas) **BISD notifies parents of 15,000 students of data breach.** The superintendent of schools for Beaumont Independent School District (BISD) in Beaumont, Texas, September 8 announced letters are being mailed to parents of nearly 15,000 of its 19,848 students to inform them of a potential recent data breach. According to the superintendent, the breach concerning confidential information that was placed on the staff server for principals to access was discovered September 2. The posted data was about potential student success on future state academic assessments. Inadvertently, private information—including the name, date of birth, gender, Social Security number, grade and scores on the Texas Assessment of Knowledge and Skills exam of students who were in the third through 11th grades during the 2009-2010 school year — were potentially exposed. When BISD officials learned of the breach, its technology team moved to secure the files and expunge the data from outside accessibility, including Internet search engines. The team implemented additional strategies to further protect BISD from future potential data breaches.
Source: http://www.kfdm.com/news/data-44672-breach-bisd.html

40. *September 7, Marysville Appeal-Democrat* – (California) **Cleanup focuses on solvent at Beale.** A plan to clean up contaminated groundwater in and around Beale Air Force Base near Marysville, California should be in place later this year, according to officials hosting a meeting September 7 on the topic. Three locations, out of 18 identified, have levels of a solvent, trichloroethylene (TCE), used at the base during World War II and the 1950s, but largely abandoned since then. TCE is dangerous mostly if inhaled. And testing on wells near the base show levels below the minimum safe level of one part per billion, an official said. Within 5 years, he said, work should begin on all 18 groundwater contamination sites around the base. The solvents came from fuel storage or spillage. Base and state officials learned of the problem in 1984 when a new law put the base out of compliance for safe levels of TCE and other solvents.
Source: http://www.appeal-democrat.com/news/solvent-109746-beale-clean.html

For more stories, see items **1**, **5**, **13**, **14**, **15**, **23**, and **58**

[Return to top]

Emergency Services Sector

41. *September 8, Redmond Patch* – (Washington) **Suspected hackers send police team to house of Microsoft employee.** Sammamish, Washington police rushed to the home of Microsoft employee the week of August 29 in response to a report of a problem after the King County Sheriff's Office received a 911 call from AT&T. The AT&T Emergency Instant Message Relay (AEIMR) system, a police report said, had received an instant message from a male which read, "2 armed Russian males broke in and they shot my son. They have Claymores outside â□¦ my door is barricaded â□¦ pls hurry!" The AEIMR asked the male for a phone number and he replied, "they cut the phone lines." A team of sheriff's deputies arrived at the house at 4:10 a.m. The operator was able to make contact with a man in the house who said he was all right. He believed this was a hoax by hackers, because similar false calls had happened to Microsoft employees, the police report said. The man explained he works with Xbox Live Operations. One of his duties, he said, is to head a team that tracks and shuts down hackers who attempt to exploit the system. Hackers, he told police, have been known to retaliate.
Source: http://redmond.patch.com/articles/suspected-hackers-send-police-team-to-house-of-microsoft-employee

42. *September 8, Arizona Republic* – (Arizona; International) **Guard troops at Arizona border to stay additional 90 days.** The U.S. President's administration said September 8 that 1,200 National Guard troops will remain on watch for drug traffickers and illegal immigrants in Arizona and other states neighboring Mexico for an additional 90 days. This is the second time the Administration has extended the National Guard's temporary deployment, which originally was scheduled to end in June. The troops have been stationed along the border since summer 2010. They primarily provide support to the Border Patrol and other law-enforcement agencies. The temporary deployment was scheduled to end June 30, but was extended until September 30, the end of the federal government's fiscal year. The troops will now remain until the end of December, said a spokesman at the Office of the Secretary of Defense.
Source:
http://www.azcentral.com/arizonarepublic/news/articles/2011/09/08/20110908arizona-guard-trooops-stay-extended.html

43. *September 8, Associated Press* – (California) **Contra Costa pays $1.5m over hospital shooting.** Contra Costa County, California will pay nearly $1.5 million to settle a lawsuit over the death of a knife-waving man who was shot by sheriff's deputies in an emergency room. The Contra Costa Times said the settlement was approved by county supervisors in July, and reported last month. The 47-year-old of Rio Vista was shot by deputies in 2009 as he waved a pocketknife he was using to cut his restraints in the emergency room at Contra Costa Regional Medical Center. He had checked himself into the Martinez hospital for treatment of alcohol withdrawal symptoms, and was agitated. His four children filed a federal wrongful-death lawsuit last year. They

claimed deputies used excessive force.
Source: http://www.sacbee.com/2011/09/08/3893259/contra-costa-pays-15m-over-hospital.html

44. *September 8, IDG News Service* – (National) **LightSquared faces Congress, amends LTE plan.** LightSquared's proposed 4G mobile network on satellite frequencies would hinder hurricane and tornado tracking, earthquake reporting, and the prediction of floods and volcanic eruptions, federal officials told Congress September 8. The company and its proposed hybrid satellite-LTE (Long-Term Evolution) network came under sometimes harsh questioning during a hearing before the House Committee on Science, Space, and Technology, with some members calling for a compromise solution to the conflict between LightSquared and the GPS (Global Positioning System) industry. Tests earlier this year showed LightSquared's ground-based network would cause major interference with GPS in the upper part of the company's spectrum. Debate is now swirling around whether the network could operate in its lower frequencies without causing problems.The impact would extend to weather forecasting, including hurricane and tornado tracking, because the satellites and ground-based systems used for those purposes rely on GPS, said the deputy under secretary of the National Oceanic and Atmospheric Administration. In addition, the U.S. Geological Survey would have problems predicting floods, landslides, and even volcanic eruptions because of equipment such as stream gauges that rely on GPS, according to the associate director of natural hazards at that agency. In addition to causing problems with the Federal Aviation Administration's (FAA) next-generation air traffic control system, interference with GPS would probably affect emerging systems to prevent collisions in the rail system and highways, a representative of the Department of Transportation told the committee. An earlier FAA analysis reportedly had predicted nearly 800 additional deaths from air crashes if the network were built.
Source:
http://www.computerworld.com/s/article/9219874/LightSquared_faces_Congress_amends_LTE_plan

For more stories, see items **1**, **31**, and **52**

[Return to top]

Information Technology Sector

45. *September 9, H Security* – (International) **Microsoft and Adobe preview September Patch Tuesday.** When it releases its monthly patches September 13, Microsoft will publish five bulletins categorized as "important" to close 15 holes. Most of the bulletins fix vulnerabilities in Microsoft Office, which attackers can use to inject malicious code and escalate rights. Arbitrary code can also be executed in the Mac edition of Office, and rights can also be escalated in the server component SharedPoint Workspace. One bulletin closes a hole in all Windows versions starting with XP (including Server) that attackers can use to remotely inject code. It is currently unclear why Microsoft does not categorize this bulletin as "critical." In addition, Microsoft will fix a privilege escalation problem in Windows Server from version 2003. Finally, the Windows

Malicious Software Removal Tool will receive current virus signatures. September 13 is also Adobe's patch day. The company announced it will be closing critical holes in all currently maintained versions of Adobe Reader and Acrobat both for Windows and Mac. Adobe also announced it was working to remove compromised DigiNotar-CA certificates from its products. For the time being, Adobe published a workaround for users who do not want to wait for the official update.
Source: http://www.h-online.com/security/news/item/Microsoft-and-Adobe-preview-September-Patch-Tuesday-1340099.html

46. *September 9, H Security* – (International) **Anonymisation service uses botnet as proxies.** Anonymization service AWM Proxy rents computers infected with the TDL4 bot for use as proxies, according to a report by a security expert. Starting at $3 per day, users can have their data traffic directed through the bot network to surf the Internet anonymously with other people's IPs. The researcher said the provider has been in business since the beginning of 2008. A Firefox extension reportedly facilitates configuration and use. The firm said it does not save any log files about its users' activities. If the proxy user views illegal content, or uses the anonymized connection to spread terror threats, the owner of the infected system could face legal consequences. To prove they did not commit these illegal actions themselves, they will first have to find the rootkit deep down in their system. Among other things, it implements its own encrypted file system; its rootkit functions even work on 64-bit Windows. However, the proxy module is only one of the bot's functions. Once the virus has settled down in a user's system, the botnet operator can load and execute files on an infected computer — so TDL4 can be used to send spam or in DDoS attacks. Online banking sessions might also be vulnerable.
Source: http://www.h-online.com/security/news/item/Anonymisation-service-uses-botnet-as-proxies-1339950.html

47. *September 8, IDG News Service* – (International) **After digital certificate hack, Mozilla seeks reassurances.** Following the hack of DigiNotar, Mozilla is asking issuers of digital certificates to take a look at their internal security and to report back in a week. In e-mails sent out to digital certificate authorities September 8, Mozilla's Certificate Authority (CA) Certificates Module owner asked CAs such as Symantec and Go Daddy to audit their systems for any possible compromise, confirm that nobody can issue a digital certificate without two-factor authentication, and shore up practices with third parties that might be able to issue digital certificates using the CA's root key. Mozilla is giving CAs until September 16 to respond, but the browser maker is not saying what will happen if any of its 54 CAs ignore the request. Mozilla is also telling the CAs to put "automatic blocks in place for high-profile domain names (including those targeted in the DigiNotar and Comodo attacks this year)," Mozilla's CA Certificated Module owner wrote in the e-mail. "Please further confirm your process for manually verifying such requests, when blocked," she wrote. By asking for a manual verification, Mozilla is trying to make it harder for anyone to issue a digital certificate for Google.com or Facebook.com, two domains that were targeted in the DigiNotar hack.
Source:

http://www.computerworld.com/s/article/9219860/After_digital_certificate_hack_Mozilla_seeks_reassurances

48. *September 8, threatpost* – (International) **Adobe says it is breaking ties to Diginotar.** Adobe said September 8it was removing Diginotar's Qualified CA certificate from the Adobe Approved Trust List, according to a company blog post. The move would affect Adobe Reader and Adobe Acrobats Versions 9 and X. It is the latest move by major software vendors to break ties to the compromised, Dutch certificate authority, which was found to have unwittingly issued hundreds of fraudulent certificates in the names of prominent organizations in recent months. In a post on the company's Product Security Incident Response Team (PSIRT) blog, Adobe said it hoped to have implemented the change by September 9. The company provided instructions for removing Diginotar certificates from the Approved Trust List manually. Those instructions are available on the PSIRT blog.
Source: http://threatpost.com/en_us/blogs/adobe-says-it-breaking-ties-diginotar-090811

49. *September 8, Wired* – (International) **Researchers' typosquatting stole 20 GB of e-mail from Fortune 500.** Two researchers who set up doppelganger domains to mimic legitimate domains belonging to Fortune 500 companies said they managed to steal 20 gigabytes of misaddressed e-mail over 6 months. The intercepted correspondence included employee usernames and passwords, sensitive security information about the configuration of corporate network architecture that would be useful to hackers, affidavits and other documents related to litigation in which the companies were embroiled, and trade secrets, such as contracts for business transactions. Doppelganger domains are ones that are spelled almost identically to legitimate domains, but differ slightly, such as a missing period separating a sub-domain name from a primary domain name. The researchers found that 30 percent, or 151, of Fortune 500 companies were potentially vulnerable to having e-mail intercepted by such schemes, including top companies in consumer products, technology, banking, Internet communication, media, aerospace, defense, and computer security. The researchers also discovered that a number of doppelganger domains had already been registered for some of the largest companies in the United States by entities that appeared to be based in China, suggesting that spies may already be using such accounts to intercept valuable corporate communications.
Source: http://www.wired.com/threatlevel/2011/09/doppelganger-domains/

For more stories, see items **14**, **20**, **41**, and **50**

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

50. *September 9, The Register* – (International) **Office 365, Hotmail and SkyDrive hit by outage.** Microsoft's Office 365 cloud service experienced another outage September 9. This time it had company as Hotmail and SkyDrive were also downed by the same DNS (Domain Name System) issue. Outages started around 4 a.m. GMT and lasted for around 3.5hours affecting mostly users in Asia Pacific and North America. On the official Office365 Twitter feed, Microsoft said: "Preliminary root cause suggests a DNS issue, though we're still working hard to restore." This is the second major outage since Office 365 launched in late June as the successor to BPOS. Microsoft said it has a financially backed SLA for its cloud services, and last month gave BPOS customers a 25 percent credit note on future invoices following an outage. Hotmail, Skydrive, and other Live properties were also out of service, the Inside Windows Live blog confirmed. "We are working on propagating the DNS configuration changes and so it will take some time to restore service to everyone. Again we appreciate your patience," the firm said. In a statement sent to The Register, Microsoft said DNS issues had caused service degradation for "multiple services", adding "we are conducting a review of the incident".
    Source: http://www.theregister.co.uk/2011/09/09/microsoft_cloud_outage/

For more stories, see items **15**, **44**, **47**, and **49**

[Return to top]

Commercial Facilities Sector

51. *September 8, Fairfield Minutemean* – (Connecticut) **Police arrest Fairfield man in arson spree.** Fairfield, Connecticut police announced September 8 they arrested a 34-year-old Fairfield man in connection with a series of arsons at vacant houses between September 5 and September 8. Between those dates, fire and police department personnel responded to six late night, residential arson fires. The homes appeared to have been targeted because they were vacant and/or were for sale, police said. Several of the homes were extensively damaged, and in one case, a firefighter was hospitalized with burns he suffered while battling the fire. The man arrested is also a suspect in several fires in nearby municipalities.
    Source:
    http://www.minutemannewscenter.com/articles/2011/09/08/fairfield/news/doc4e6979ec9956b796782272.txt?viewmode=fullstory

52. *September 8, Milwaukee Journal-Sentinel* – (Wisconsin) **Pool chemicals sicken 3 Wis. firefighters.** Six people, including three firefighters, were taken to the hospital September 8 after a pool pump malfunctioned at Gold's Gym in Hales Corners, Wisconsin. The Hales Corners Fire Department received a call shortly before 9 a.m. about a possible chemical spill or leak. Investigation showed a pool pump had malfunctioned and stopped operating. Once it started to back up, it sent out more than its normal dose of chlorine and acid, and people who breathed the cocktail suffered

respiratory symptoms, the fire chief said. The gym was evacuated, and firefighters ventilated the room and monitored air quality. All firefighters had been released from the hospital by the afternoon. The other patients were released later in the day.
Source: http://www.firehouse.com/topic/strategy-and-tactics/pool-chemicals-sicken-3-wis-firefighters

For more stories, see items **1**, **3**, **6**, **25**, **29**, **35**, **49**, **53**, and **57**

[Return to top]

National Monuments and Icons Sector

53. *September 9, Associated Press* – (Texas) **Biggest air assault yet set for Texas blaze.** Firefighters were planning a major aerial assault September 9 of a massive wildfire that has raged for days across Central Texas, destroying almost 1,400 homes and tens of thousands of acres of drought-parched land. Officials planned to deploy a converted DC-10 jetliner capable of dropping 12,000 gallons of fire retardant on the fire and smoldering hotspots across some 45 square miles. Crews were making steady progress against the fire burning in and around Bastrop, closing in around its biggest flames. Concern lingers, however, about wind sparking flare-ups or fanning flames outside the area. The DC-10, one of the nation's largest firefighting jets, is just one more strategy the community unfamiliar with massive wildfires is employing to finally get control of the fire. The blaze has been the most catastrophic of nearly 180 wildfires that the forest service said erupted across Texas the week of September 5. The outbreak has left nearly 1,700 homes statewide in charred ruins, killed four people, and forced thousands of people to evacuate.
Source: http://news.yahoo.com/biggest-air-assault-yet-set-texas-blaze-073135078.html

54. *September 8, KMGH 7 Denver* – (Colorado; National) **9 million pot grow removed near Deckers.** Local and federal authorities said they found about 3,000 marijuana plants in the Pike National Forest in Colorado with a street value of $9 million. The U.S. Forest Service (USFS) and the Douglas County sheriff's office said September 8 no one has been arrested in connection with the illegal grow operation southwest of Denver. Crews from the Colorado National Guard helped fly the plants out of the forest and dismantled a drip irrigation system for the crop. The Douglas County Sheriff's Office, USFS, Colorado National Guard, U.S. Drug Enforcement Administration, and the South Metro Drug Task Force worked on the investigation. A USFS special agent said large-scale marijuana operations have been found in Colorado over the last 3 years and are believed to be connected to illegal grows that have spread on public lands in California, Oregon, Washington, Idaho, and Utah.
Source: http://www.thedenverchannel.com/news/29125776/detail.html

55. *September 8, KPTV 12 Portland* – (Oregon) **Yamhill National Forest pot bust.** The Yamhill County Interagency Narcotics Team in Oregon arrested three men in connection to a rural marijuana grow September 6 in the Yamhill County National Forest. The grow was located by a detective with the narcotics team during an aerial flight. During surveillance conducted on the grow, officers witnessed three males

working in the marijuana field. A 48-year-old man, a 35-year-old man, and a 39-year-old man were arrested for unlawful manufacture, delivery, and possession of marijuana. Officers found 569 mature marijuana plants valued around $550,000. Detectives believe the large grow operation is linked to a drug trafficking organization. The narcotics team was assisted by the Oregon State Police, Yamhill County Sheriff's Office, McMinnville Police Department, the U.S. Bureau of Land Management, and regional narcotics teams from Tillamook, Polk, and Lincoln counties.
Source: http://www.kptv.com/story/15422971/yamhill-national-forest-pot-bust

56. *September 8, Associated Press* – (District of Columbia) **2 injured dismantling crane at National Cathedral.** Two workers were injured September 8 at the National Cathedral in Washington D.C. as they were dismantling a crane that collapsed on the grounds a day earlier. A Cathedral spokesman said two men were taken away by ambulance. It was not clear what caused the injuries or how severely the men were injured. An investigation is under way to determine what caused the massive crane to topple over September 7. It had been brought in to repair earthquake damage.
Source: http://news.yahoo.com/2-injured-dismantling-crane-national-cathedral-213028319.html

[Return to top]

Dams Sector

57. *September 9, Associated Press* – (Pennsylvania) **Susquehanna River crests below levees in NE Pa.** The Susquehanna River crested above 38 feet, but below the top of the levee system protecting tens of thousands of residents in northeastern Pennsylvania, the National Weather Service (NWS) said early September 9. Thousands living in riverfront communities with no flood protection endured catastrophic flooding that led to some rescues. A broken gauge at Wilkes-Barre prevented experts from determining the exact crest, according to a NWS hydrologist, who added officials were confident the river will not go back up because the waterway has already crested in upstream communities. As many as 75,000 residents in Wilkes-Barre and surrounding communities remain under a mandatory evacuation. Rain from Tropical Storm Lee pounded the state earlier the week of September 5, not long after Hurricane Irene soaked the same areas. The U.S. President declared a state of emergency in Pennsylvania September 9, clearing the way for federal aid. The Pennsylvania Emergency Management Agency said 14 wastewater treatment plants had been taken offline by flooding, and residents were urged to stay away from flood waters over concerns about toxicity. In West Pittston, north of Wilkes-Barre and unprotected by the levees, several hundred homes were underwater. A Columbia County public information officer said about a quarter of Bloomsburg is affected by floodwaters and several homes were swept off their foundations by the rushing waters. There was flooding in other parts of the state, including along the Delaware River, which crested in Easton and Riegelsville at around 5:15 a.m., according to the National Weather Service. Hundreds of roads across the eastern half of the state were closed by flooding. A nearly 40-mile stretch of the Pennsylvania Turnpike closed September 8 because rising waters threatened a bridge in Dauphin County, but the turnpike reopened in time

for the September 9 morning rush hour after water levels dropped.
Source: http://www.deseretnews.com/article/700177544/Susquehanna-River-crests-below-levees-in-NE-Pa.html?pg=2

58. *September 8, Reading Eagle* – (Pennsylvania) **Army Corps of Engineers releasing water from Blue Marsh.** The U.S. Army Corps of Engineers started a controlled release of water from the Blue Marsh Reservoir in Reading, Pennsylvania in an effort to prevent water from overflowing uncontrolled into the Schuylkill River, the Reading Eagle reported September 8. "If we release water we know how much water is flowing downstream," said the Blue Marsh park manager. "If it goes over the spillway, we have no way of knowing how much water is flowing downstream. Whether it overflows depends on the inflow into the reservoir, and so far the inflow has been phenomenal," he added. State police closed Route 183 from Route 222 to Interstate 78. Hydrologists from the U.S. Geological Survey who monitor river gauges on the Schuylkill said the river rose 6 inches in less than 1 hour September 8. The river water was near the top of berms along the banks at Reading Area Community College at 11 a.m.
Source: http://readingeagle.com/article.aspx?id=330997

For more stories, see items **9**, **23**, and **44**

[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