Homeland Security

Daily Open Source Infrastructure Report 21 September 2012

Top Stories

- An underground utility explosion shut down streets and forced evacuations of many office buildings and a courthouse in Albany, New York. – *Albany Times-Union* (See item **1**)
- Researchers discovered new versions of a zero-day vulnerability in Internet Explorer targeting defense contractors, including a U.S. aircraft and weapons delivery systems firm and a U.S. aerospace and defense technology company. – *Infosecurity* (See item **7**)
- A financial services industry group warned U.S. banks, brokerages, and insurers to be on heightened alert for cyber attacks after Bank of America and JPMorgan Chase experienced unexplained outages on their public Web sites. – *Reuters* (See item **10**)
- Washington D.C. train riders experienced massive delays after a power failure stopped a train carrying 1,000 people in a tunnel between two stations. – *WTOP 103.5 FM Washington, D.C.* (See item **19**)
- The piece of malware known as ZeroAccess was found to be present on more than 1 million computers spread throughout almost 200 countries. – *Softpedia* (See item **41**)

Fast Jump Menu

PRODUCTION INDUSTRIES

• Energy
• Chemical
• Nuclear Reactors, Materials and Waste
• Critical Manufacturing
• Defense Industrial Base
• Dams

SUSTENANCE and HEALTH

• Agriculture and Food
• Water
• Public Health and Healthcare

SERVICE INDUSTRIES

• Banking and Finance
• Transportation
• Postal and Shipping
• Information Technology
• Communications
• Commercial Facilities

FEDERAL and STATE

• Government Facilities
• Emergency Services
• National Monuments and Icons

Energy Sector

1. *September 20, Albany Times-Union* – (New York) **A big blast from below.** An underground utility explosion rocked a downtown neighborhood of Albany, New York, September 19, sending manhole covers flying with a fireball in the air. The explosions forced officials to shut down streets and several office buildings on North Pearl Street were evacuated. The blast happened at the corner of Steuben and Pearl streets, according to the fire chief. The city ordered the evacuations of buildings on North Pearl Street between State and Columbia streets. Some buildings on Eagle and Pine streets were also closed. National Grid crews were on the scene, dealing with the aftermath of the utility fire. The company cut electrical service to many downtown buildings. The mayor said the city and utility companies will need to look into the infrastructure under the ground to determine if there are widespread problems. The Albany County Judicial Center was evacuated and closed. County officials said a fire in the sewer system outside the building caused smoke to be drawn into the building's air intake system. A spokesman for National Grid said the explosion was caused by a fault on an electrical cable. He said utility crews were working to make repairs and were testing for natural gas fumes.
   Source: http://www.timesunion.com/local/article/Albany-courthouse-evacuated-roads-closed-3877873.php

2. *September 19, Associated Press* – (Ohio) **Rail cars collide in Ohio coal mine, injuring 5.** Two rail cars that transport miners collided in a southeast Ohio coal mine, sending five men to the hospital, the Associated Press reported September 19. It is unclear how seriously the miners were injured or what caused the collision at Buckingham Coal mine in Corning, about 55 miles southeast of Columbus in the area of Wayne National Forest. The Perry County deputy said two of the men were flown by medical helicopter to a hospital. He said three others were taken to other hospitals. The mine's general superintendent said the collision will be investigated.
   Source: http://www.pal-item.com/article/20120919/UPDATES/120919007/Rail-cars-collide-Ohio-coal-mine-injuring-5?odyssey=tab|topnews|text|FRONTPAGE&nclick_check=1

3. *September 19, Mankato Free Press* – (Minnesota) **Tanker rollover spills 100 gallons of gas near Le Sueur.** About 100 gallons of gasoline were spilled September 19 when a semi tanker turning into the Le Sueur, Minnesota rest area tipped over. The tanker was southbound on Highway 169 when the driver attempted to make a left turn into the rest area, a State patrol report said. He lost control and the tanker rolled over into a ditch. One lane of traffic was closed on the highway while firefighters, an emergency crew from the Minnesota Pollution Control Agency (MPCA) and law enforcement officers dealt with the crash. West Central Environmental Consultants responded to deal with the leaking fuel. An MPCA emergency crew also responded to oversee the cleanup and conduct environmental testing. Le Sueur firefighters sprayed foam on the tanker as a precaution. The rest area was closed but has since been re-opened.
   Source: http://mankatofreepress.com/local/x1023296518/Update-Tanker-rollover-spills-100-gallons-of-gas-near-Le-Sueur

For more stories, see items **7** and **47**

[Return to top]

Chemical Industry Sector

See item **27**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

4. *September 20, Nuclear Street* – (Washington) **DOE declares Hanford F Reactor first at site to be fully remediated.** The Department of Energy (DOE) announced September 19 that the first of nine Cold War-era plutonium production reactors at the Hanford Site in Hanford, Washington, has been completely cleaned up. While five other reactors have also been sealed up, the DOE reported that the F Reactor was the first to have all of its associated waste sites and ancillary buildings remediated. Operations at the F Reactor from 1954 to 1965 left behind tainted soil and buried debris that included drums, effluent pipelines, spent nuclear fuel, and other high-dose irradiated items. Contractor Washington Closure Hanford disposed of 1.5 million tons of contaminated material, most of which was sent to the Environmental Restoration Disposal Facility at the site. A total of 88 waste sites required cleanup within the 2-square-mile F Area.
   Source: http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2012/09/20/doe-declares-hanford-f-reactor-first-at-site-to-be-fully-remediated-092002.aspx

[Return to top]

Critical Manufacturing Sector

5. *September 20, WJBK 2 Detroit; Associated Press* – (Michigan) **Chrysler employee kills co-worker at Detroit factory, turns gun on self at Belle Isle.** Two people were dead following a stabbing at a Chrysler plant in Detroit September 20. Police said a man was stabbed inside the factory and later died after being taken to a hospital. The suspect fled the factory and was later found at Belle Isle park where he committed suicide. No other employees were injured, and workers on the first shift were sent home, said a spokeswoman at Chrysler Group. The Jefferson North plant employs just more than 3,000 workers on two shifts. Chrysler's senior vice president of manufacturing said the second shift was canceled for September 20.
   Source: http://www.myfoxdetroit.com/story/19593495/worker-cousin-fatally-stabbed-inside-detroit-chrsyler-factory

[Return to top]

Defense Industrial Base Sector

6. *September 20, Global Security Newswire* – (National) **NNSA expands nuclear arms data collection, auditors say.** The U.S. National Nuclear Security Administration (NNSA) expanded its collection of information for identifying physical problems in the nation's nuclear weapons, the Energy Department's inspector general concluded in a new report. Steps have been taken to address "gaps" in stockpile surveillance information that the semiautonomous Energy Department branch identified 2 years ago as obstacles to an initiative to step up the pace of oversight efforts, according to the assessment. The agency increased its collection of such data by "increasing funding and expanding laboratory tests," the paper states. The heads of U.S. nuclear weapons laboratories "expressed concerns in their annual assessments about gaps of surveillance data due to a reduction in laboratory tests," the document says. The atomic agency in fiscal 2011 "increased surveillance funding within the Directed Stockpile Work program by $58 million," auditors wrote. The move allowed for a "142 percent increase (from 24 to 58 tests) in laboratory tests," as well as other oversight changes, according to the report. "NNSA plans to continue funding the surveillance program at or above the [fiscal year] 2011 level for future years," it adds. "According to a senior NNSA official, the laboratory directors assured NNSA that the proposed out-year funding will be sufficient to perform surveillance activities to affirm confidence in the stockpile."
Source: http://www.nti.org/gsn/article/us-expands-nuclear-arms-data-collection-auditors/

7. *September 19, Infosecurity* – (International) **Internet Explorer zero-day targeting defense industry.** Researchers at AlienVault discovered new versions of the new zero-day vulnerability in Internet Explorer that are targeting a number of defense and industrial companies, including a U.S. aircraft and weapons delivery systems firm, a U.S. aerospace and defense technology company, and a U.K. defense contractor. "We also found a fake domain of a company that builds turbines and power sources used in several applications including utilities and power plants," a researcher said. "We were able to check that the official Web site of the company has been compromised as well and it is serving the Internet Explorer ZeroDay to the visitors. They've included an iframe to the exploit in the entry page." The researcher and his team also found the exploit code evolved and is now able to infect not only Windows XP but also Windows 7 32-bit running Java 6.
Source: http://www.infosecurity-magazine.com/view/28357/

[Return to top]

Banking and Finance Sector

8. *September 20, Softpedia* – (Puerto Rico; National) **Tax refund fraud scheme shut down after U.S. authorities arrest 14 suspects.** September 19, authorities arrested 14 individuals suspected of participating in one of the largest and longest stolen identity tax refund fraud schemes the United States has ever witnessed. It is believed that the fraudsters attempted to steal around $65 million. The individuals caused damages of

$11.3 million according to a U.S. attorney's office in New Jersey. They were charged with conspiracy to defraud the State and theft of government property. The perpetrators would steal the Social Security numbers, dates of birth, and other sensitive details of unsuspecting individuals, many of whom reside in Puerto Rico. The fraudulently obtained data would then be utilized to file Individual Income Tax Returns. The tax return checks issued by the U.S. Department of the Treasury were intercepted by the conspirators, often by bribing mail carriers.
Source: http://news.softpedia.com/news/Tax-Refund-Fraud-Scheme-Shut-Down-After-US-Authorities-Arrest-14-Suspects-293640.shtml

9. *September 20, Softpedia* – (International) **Chase Bank site suffers outage, Muslim hackers take credit.** After the public-facing Web site of Bank of America (BoA) experienced some minor outages, JPMorgan Chase suffered from similar problems, Softpedia reported September 20. The same hackers who attacked BoA also took responsibility for taking down Chase.com. On September 18, a hacker collective threatened to attack the Web sites of BoA and the one of the New York Stock Exchange in protest against a controversial film. At the time, they threatened that other organizations would also be targeted in the upcoming days, and Chase appears to be one of them. "Chase.com is experiencing intermittent issues. We're working to restore full connectivity and apologize for any inconvenience," read a message posted by the financial institution on Twitter. Around 5 hours later, the company announced that the site was back online. The "Cyber fighters of Izz ad-din Al qassam" published a second Pastebin document, taking credit for the outage.
Source: http://news.softpedia.com/news/Chase-Bank-Site-Suffers-Outage-Muslim-Hackers-Take-Credit-293681.shtml

10. *September 20, Reuters* – (International) **Bank group warns of heightened risk of cyber attacks.** The Financial Services Information Sharing and Analysis Center (FS-ISAC) warned U.S. banks, brokerages, and insurers September 19 to be on heightened alert for cyber attacks after Bank of America and JPMorgan Chase experienced unexplained outages on their public Web sites. FS-ISAC raised the cyber threat level to "high" from "elevated" in an advisory to members, citing "recent credible intelligence regarding the potential" for cyber attacks as its reason for the move. The move by FS-ISAC came just 2 days the FBI published a "fraud alert" advising financial services firms that cyber criminals may be disrupting service to their Web sites in a bid to keep banks from noticing a recent surge in fraudulent large-sized wire transfers.
Source: http://in.reuters.com/article/2012/09/20/us-jpmorganchase-website-idINBRE88I16M20120920

11. *September 20, WCVB 5 Boston* – (Massachusetts; Rhode Island) **Police: 'Bearded Bandit' bank robber arrested at Seekonk motel.** A man believed to be the "Bearded Bandit" was arrested in Seekonk, Massachusetts. Police arrested the man September 19 at the Seekonk Motel 6 where he had been living, according to police. The arrest came after an officer spotted two vehicles in the motel parking lot that matched descriptions of getaway cars used in at least eight robberies in Rhode Island and Massachusetts. Investigators said the man was clean shaven and a fake beard was found inside his room.

Source: http://www.wcvb.com/news/local/boston-south/Police-Bearded-Bandit-bank-robber-arrested-at-Seekonk-motel/-/9848842/16673050/-/ccmhhe/-/index.html

12. *September 19, U.S. Federal Bureau of Investigation* – (International) **Former CME Group software engineer pleads guilty to stealing Globex computer trade secrets while planning to improve electronic trading in China.** A former senior software engineer for Chicago-based CME Group Inc. pleaded guilty September 19 to theft of trade secrets for stealing computer source code and other proprietary information while at the same time pursuing plans to improve an electronic trading exchange in China. The defendant admitted that he downloaded more than 10,000 files containing CME source code that made up a substantial part of the operating systems for the Globex electronic trading platform. The government maintains that the potential loss was between $50 million and $100 million, while the defendant maintains that the potential loss was less than $55.7 million. The programmer, who worked for CME Group for 11 years, pleaded guilty to two counts of theft of trade secrets. The programmer and two unnamed business partners developed plans to form a business that would contract to the Zhangliagang chemical electronic trading exchange to increase trading value on the exchange using the stolen code.
Source: http://www.fbi.gov/chicago/press-releases/2012/former-cme-group-software-engineer-pleads-guilty-to-stealing-globex-computer-trade-secrets-while-planning-to-improve-electronic-trading-in-china

13. *September 19, WAPT 15 Jackson* – (Mississippi) **Bond set for women accused in robbery attempt with fake bomb.** Bond was set for two women accused in a fake bomb plot in Canton, Mississippi,September 19, officials said. Canton police said a woman who claimed that two men forced her to strap on a backpack with what she thought was explosives was charged with bank robbery. Investigators said she walked into a Trustmark bank September 14 and told employees she had a bomb in the backpack she was wearing. She told police that two men attacked and kidnapped her from a gas station and forced her to strap on the backpack that she believed contained explosives. They then threatened to kill her if she did not rob the bank, police said. Initially, police said it appeared she had been a victim, but the investigation later led to her arrest. Police did not say what role they believed the second woman played in the robbery attempt. Police said the backpack contained two bricks, and no explosives.
Source: http://www.wapt.com/news/central-mississippi/Court-next-stop-for-women-accused-in-fake-bomb-robbery-attempt/-/9156946/16659322/-/f1rgsiz/-/index.html

For more stories, see items **42** and **46**

[Return to top]

Transportation Sector

14. *September 20, Philadelphia Inquirer* – (Pennsylvania) **20 children sent to hospital after school bus crash.** Twenty children were taken to a hospital following a crash September 20 between a school bus and a car in northeast Philadelphia. The injuries were not serious, medics reported. The crash occurred at Roosevelt Boulevard and

Adams Avenue.
Source:
http://www.philly.com/philly/news/breaking/20120920_Schook_bus_crash_sends_14_children_to_hospital.html

15. *September 20, WPTV 5 West Palm Beach* – (Florida) **Judge orders St. Lucie school bus driver in deadly crash pay fine, suspends license.** A former St. Lucie County, Florida School District bus driver September 19 publicly apologized for the first time for the bus crash that killed one student and injured others in March, WPTV 5 West Palm Beach reported September 20. He pleaded no contest to the traffic citation that the Florida Highway Patrol filed after investigating the accident at Okeechobee and Midway roads. At the end of the hearing, the driver was given the minimum required by law in a fatal accident: a $1,000 fine and a 6-month license suspension.
Source: http://www.wptv.com/dpp/news/region_st_lucie_county/albert-hazen-judge-orders-st-lucie-school-bus-driver-in-deadly-crash-pay-fine-suspends-license

16. *September 20, St. Louis Post-Dispatch* – (Illinois) **Mississippi River traffic moving again near Granite City.** Mississippi River traffic was moving again September 20 after busy Lock 27 was reopened near Granite City, Illinois. Damage to a structure protecting the busy lock on the Chain of Rocks Canal had brought commercial barge traffic to a standstill on the upper Mississippi River as crews made emergency repairs. The Coast Guard was working to organize vessels and cargo to get through the lock in the best order based on various factors. A Coast Guard lieutenant expected it to take up to 3 days before traffic flow was back to normal. By the time the lock reopened, there were 63 vessels, with a total of 455 barges, backed up and waiting to pass. Officials had let 6 vessels with 80 barges through. The damaged barrier, a large cylindrical cell, was discovered September 15 after rock spilled out of it near the opening of the lock. Precariously low water levels on the river had exposed one of the less-fortified sections of the cell. It is unclear how the protection cell was damaged.
Source: http://www.stltoday.com/news/local/metro/mississippi-river-traffic-moving-again-near-granite-city/article_0ceb936a-39ad-5da0-b12f-84824960be17.html

17. *September 20, Trucking Info* – (Kansas) **FMCSA shuts down Kansas trucking company for extreme hours of service violations.** The Federal Motor Carrier Safety Administration (FMCSA) ordered Kansas-based commercial truck company HP Distribution LLP and an affiliated company, HP Distribution LLC, to immediately cease all transportation services based on serious hours-of-service and other safety violations that posed an imminent hazard to public safety, Trucking Info reported September 20. FMCSA immediately placed HP Distribution, its vehicles and drivers, out of service after agency investigators found a range of serious safety violations. Investigators found the company knowingly permitted its drivers to falsify the number of hours they operated the vehicle in an attempt to conceal hours-of-service violations. Additionally, HP Distribution dispatched potentially fatigued drivers on interstate trips without regard for the safety of the drivers or the traveling public. According to the government order, the company has a history of non-compliance and violations of Federal Motor Carrier Safety Regulations.
Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=78074

18. *September 20, Manassas News & Messenger* – (Virginia) **Remains found along Manassas Park VRE tracks not human.** The remains found September 19 along the Virginia Railway Express (VRE) railroad tracks near Manassas Drive that shut down trains for several hours were found not to be human. A Manassas Park police spokeswoman said a medical examiner confirmed September 20 that the remains, found inside a suspicious package, were not human. The investigation shut down the rails and left thousands of commuters stranded for hours September 19. All train traffic was stopped south of the Burke, Virginia station and many VRE passengers were stuck on their trains. VRE officials dispatched buses to the Burke and Clifton stations to help get stranded passengers home, and turned around at least one train, tracking it back to Alexandria. Cabs and buses were called in to help get the estimated 1,500 to 1,700 stranded commuters back home. Vehicle traffic in the area was also backed up for hours on Manassas Drive and Euclid and Liberia avenues. Trains began running again 4 hours after the shutdown.
Source: http://www2.insidenova.com/news/2012/sep/20/remains-found-along-manassas-park-vre-tracks-not-b-ar-2220356/

19. *September 19, WTOP 103.5 FM Washington, D.C.* – (Maryland; Washington, D.C.) **Red Line running again after train stuck in tunnel.** Washington Metropolitan Area Transit Authority (WMATA) riders experienced residual delays on the Red Line in Washington D.C. after a power failure September 19 stopped a train in the tunnel between the Friendship Heights and Tenleytown-AU stations with roughly 1,000 people on board. Red Line trains were traveling at 35 mph until the transit agency could determine what caused the problem. The issue that disabled the train forced riders to stay on board for about an hour. During that time, Metro kept the train in the tunnel until it reestablished power. The outage occurred on Wisconsin Avenue outside the Tenleytown-AU station, according to Metropolitan police. Metro closed the station during the incident. It has since reopened.
Source: http://www.wtop.com/41/3044606/Red-Line-running-again-after-train-stuck-in-tunnel

For more stories, see items **1** and **3**

[Return to top]

Postal and Shipping Sector

20. *September 19, Des Moines Register* – (Iowa) **Pop bottle bomb found in Urbandale mailbox.** A third pop bottle bomb was found in Urbandale, Iowa, in a residential mailbox September 15, within blocks of two similar explosives discovered in July. A resident discovered remnants of the bottle bomb inside the mailbox, Urbandale police officials said. The mailbox was still intact. Pop bottle bombs were also discovered in two other residential mailboxes in July. Both were damaged in the explosion. No one has been charged.
Source: http://blogs.desmoinesregister.com/dmr/index.php/2012/09/19/pop-bottle-bomb-found-in-urbandale-mailbox/

For another story, see item **8**

[Return to top]

Agriculture and Food Sector

21. *September 20, U.S. Department of Agriculture* – (National) **USDA expands drought assistance to 22 states.** September 20, the U.S. Secretary of Agriculture announced an additional $11.8 million in financial and technical assistance to help crop and livestock producers in 22 States apply conservation practices that reduce the impacts of drought and improve soil health and productivity. The announcement expanded upon previous efforts and brought the total assistance to nearly $28 million. Funding targeted States that are experiencing either exceptional or extreme drought conditions. Exceptional drought continues to dominate sections of Arkansas, Colorado, Georgia, Iowa, Kansas, Kentucky, Missouri, Nebraska, New Mexico, Oklahoma, South Dakota, Tennessee, Texas, and Wyoming.
Source: http://www.agprofessional.com/news/USDA-expands-drought-assistance-to-22-states-170339366.html

22. *September 20, Associated Press* – (South Dakota) **South Dakota ag officials advise tests for aflatoxin levels in corn.** South Dakota agriculture officials advised farmers and ranchers to test for aflatoxin levels in their corn, distiller's grains, and silage piles due to the 2012 drought, the Associated Press reported September 20. South Dakota State University Extension educators said feed refusal, reduced growth rate, and decreased feed efficiency are the predominant signs of chronic aflatoxin poisoning in livestock. High levels of aflatoxin fed to dairy cows can lead to contamination of the milk that is produced. The National Corn Growers Association said aflatoxin is most prevalent in corn, cotton, peanuts and tree nuts.
Source: http://www.ksfy.com/story/19592742/south-dakota-ag-officials-advise-tests-for-aflatoxin-levels

23. *September 19, Food Safety News* – (National) **Spinach recalled for Listeria risk.** Kroger initiated a recall of spinach sold at locations in the midwest and eastern part of the country because the product may be contaminated with Listeria monocytogenes, Food Safety News reported September 19. The recall was issued for the Fresh Selections Tender Spinach sold in 10 oz. bags. The affected spinach was sold in Kroger stores located in Georgia, South Carolina, Alabama, Tennessee, Ohio, Indiana, Virginia, Michigan, Illinois, Missouri, North Carolina, Virginia, and West Virginia. The spinach was also sold at Jay C, Dillons, Baker's, Gerbes, Food4Less Fremont, Food4Less, and FoodsCo.
Source: http://www.foodsafetynews.com/2012/09/spinach-recalled-for-listeria-risk/#.UFsXZpH2q70

24. *September 19, U.S. Food and Drug Administration* – (National) **GHSW, LLC recalls limited quantity of expired fresh-cut mango products due to possible health risk.** September 19, the U.S. Food and Drug Administration (FDA) announced that GHSW, LLC of Houston, Texas, initiated a voluntary recall of a limited quantity of

expired products that contain fresh-cut mangoes and were distributed to retail supermarkets due to the potential risk that the mangoes may contain Salmonella. This recall is associated with Food Source's recall of mangoes sourced from Agricola Daniella. The FDA issued an import alert and advised consumers not to eat mangoes from Agricola Daniella. The products listed in this recall were distributed through retail stores in Alabama, Arkansas, Louisiana, Mississippi, and Texas. Products were packaged in clear plastic containers and were distributed to retail distribution centers August 29-September 5. Products contained printed code dates on the top or bottom labels of the plastic package ranging from September 7-September 15.
Source: http://www.fda.gov/Safety/Recalls/ucm320209.htm

For more stories, see items **27** and **50**

[Return to top]

Water Sector

25. *September 20, Elyria Chronicle-Telegram* – (Ohio) **Repair contract signed for Vermilion water well.** Vermilion, Ohio, finalized a contract with an Avon company to begin repairs on its clear well roof, the Elyria Chronicle-Telegram reported September 20. Vermilion's clear water well was found to be leaking September 7, causing the water to have a high turbidity. That prompted a week-long boil alert for residents until the city hooked up to emergency water lines. The 47-year-old roof needed repairs before the city could again use its own water. Crews began prepping concrete September 19, and repairs should be finished by the week of September 24. The well will then have to be cleaned and disinfected to Environmental Protection Agency standards before residents can again consume the water.
Source: http://chronicle.northcoastnow.com/2012/09/20/repair-contract-signed-for-vermilion-water-well/

26. *September 20, WTOP 103.5 FM Washington, D.C.* – (Maryland) **Largo water outage to last into Thursday afternoon.** The Washington Suburban Sanitary Commission (WSSC) said it could be September 20 afternoon before 267 customers in Largo, Maryland, have their water service restored. Crews were working to fix a 24-inch water main that burst September 19. WSSC said a water station would be set up for the affected customers.
Source: http://www.wtop.com/58/3046008/Pipe-break-knocks-out-water-to-267-in-Largo-Md

27. *September 20, Auburn Citizen* – (New York) **EPA strikes agreement with GE on cleanup.** The U.S. Environmental Protection Agency (EPA) announced an agreement with General Electric Co. (GE) September 19 requiring the company to take over the maintenance and replacement of treatment systems still removing pollutants from the four remaining drinking water wells within the 4.8-square-mile contaminated Superfund site stretching from Auburn to Union Springs, New York. The wells are the last of 55 private water sources that tests concluded were contaminated with vinyl chloride, trichloroethylene, and other chemical solvents originating from leaking

storage tanks at the electronic component manufacturing plant owned and operated by GE from 1951 to 1986, and by Powerex until 1990. After the contaminants were discovered, most residents within the polluted area in Aurelius, Fleming, and Springport were connected to municipal drinking water. An EPA Region 2 spokesman said the remaining wells, of which one is residential and three are agricultural, are in Aurelius. As part of the agreement, GE will also reimburse the EPA $50,000 for past costs associated with the maintenance of the wells. EPA officials previously said the cleanup could take 30 years or more to completely rid the area of pollutants, and could cost more than $20 million. The company is currently pumping millions of gallons of water from the site and trucking it to the Auburn Wastewater Treatment Plant.
Source: http://auburnpub.com/news/local/epa-strikes-agreement-with-ge-on-cleanup/article_d7b73fc0-585a-5f62-a169-8b5ed9e4c1c3.html?comment_form=true

28. *September 19, Harrison Daily* – (Arkansas) **Help find Harrison water leak; 700 to 1,000 gallons a minute.** The Harrison, Arkansas public works director noticed a major water leak estimated to be pouring more than 1 million gallons of water a day out of the system September 19. He said the leak was noticed September 17 and 18 as a larger than normal amount of water began flowing through the city’s meter. Officials estimated it to be leaking 700 to 1,000 gallons a minute. Water department personnel walked all water lines in the system, but found nothing. The director said that because the mountainous area contains karst topography, it is likely the leak is pouring into an underground cavern or similar feature and flowing underground. Thus, it could surface a long distance from the leak. Officials said that any people who notices a drop in water pressure or water flow, or who have seen an unusually wet area, should contact city officials.
Source: http://harrisondaily.com/help-find-harrison-water-leak-to-gallons-a-minute/article_bf6aee20-02a4-11e2-9f91-0019bb2963f4.html

For another story, see item **1**

[Return to top]

Public Health and Healthcare Sector

29. *September 19, Healthcare IT News* – (Kentucky) **2,500 involved in Kentucky data breach.** The Kentucky-based Cabinet for Health and Family Services notified approximately 2,500 clients September 18 that a possible employee email account breach may have resulted in the unintentional release of personally identifiable information. In July, a cabinet’s department for community based services employee responded to a phishing email sent by a hacker. Unauthorized activity on the account was identified within a half hour, and officials said the account was then disabled. Officials were not certain if confidential contents of the email account were accessed or viewed. Officials said health information on diagnoses or Social Security numbers were not on the database and therefore could not have been accessed. Names, addresses, and other ID codes were, however. The cabinet was required to notify clients individually of any potential breach by the federal Health Insurance Portability and Accountability Act. Since August 2009, the State of Kentucky has seen 14 data breaches involving the

personal health information of 76,202 patient records.
Source: http://www.healthcareitnews.com/news/2500-involved-kentucky-data-breach

[Return to top]

Government Facilities Sector

30. *September 20, KING 5 Seattle* – (Washington) **Threat of school shooting closes Western WA high school.** September 19, the Issaquah School District in Sammamish, Washington, announced Skyline High School was to be closed September 20 because of a threat of a shooting. The King County Sheriff's Office and Sammamish police were investigating the threat that stated students would be gunned down in the school's commons area. The threat said in part: "The people at that school use their wealth and social status to act superior to others and they think it makes them better. The biggest offender at the school would be the jocks. I am going to start killing them first because they deserve it the most." The threat also included a picture of an automatic gun that was to be used. The threat's author claimed the gun belonged to his father. The author went on to say he would kill until he runs out of ammunition and is killed by authorities or until he eventually takes his own life.
Source: http://www.krem.com/news/Threat-of-school-shooting-closes-Western-WA-high-school-170490506.html

31. *September 19, WSYX 6 Columbus* – (Ohio) **OSU students return to dorm after water main break.** Students living at an Ohio State University residence hall in Columbus, Ohio, were allowed back into their dorm rooms after spending more than 2 days in limbo following a water main break September 15. The water at Park-Stradley Residence Hall was not safe to drink, so the university provided students with bottled beverages. The water was expected to be deemed safe and usable within several days. Nearly 2,000 students in several buildings were evacuated after the main broke and water flooded a tunnel and sub-basements. The 1,100 residents of Park-Stradley were the last students to move back. While the students were barred from sleeping in their dorm rooms until September 19, they were able to get back inside the building September 17-18 to retrieve school supplies and clothing.
Source: http://www.abc6onyourside.com/shared/news/top-stories/stories/wsyx_osu-students-return-dorm-after-water-main-break-19734.shtml

For another story, see item **1**

[Return to top]

Emergency Services Sector

32. *September 20, NBC News* – (California) **13 inmates hurt, shots fired during 'New Folsom' prison riot.** A prisoner was shot and wounded and 12 others were sent to the hospital with "stab and slash wounds and head trauma" after a riot involving 60 inmates broke out September 19 at a prison in Folsom, California, officials said. Officers at California State Prison-Sacramento fired six bullets from a rifle during their

efforts to stop the fighting, according to a statement on the prison's Web site. "Correctional peace officers used less-than-lethal force options including blast dispersion rounds to stop the riot. Officers also discharged six rounds from the Mini 14 rifle. One inmate suffered a gunshot wound and was taken to an area hospital for treatment," the statement said. Four weapons that had been made by the inmates were found by officers. No staff members were injured. The California Department of Corrections and Rehabilitation sent a "Deadly Force Investigation Team" to investigate the use of the rifle and a review board will also conduct a "full and complete review of the incident," the statement said.
Source: http://usnews.nbcnews.com/_news/2012/09/20/13981953-13-inmates-hurt-shots-fired-during-new-folsom-prison-riot?lite

33. *September 19, Softpedia* – (National) **Conficker worm compromises prison CCTV systems.** The computers that handle the closed circuit television (CCTV) systems of an unnamed prison have been reportedly compromised by the infamous Conficker worm. The correctional institution's representatives insisted that all the necessary security measures had been set in place to block such malware, claiming that the threats identified by protection software were most likely false positives, SC Magazine noted. However, after analyzing the incident, Symantec experts discovered unpatched servers — running Windows Server 2003 — that allowed the malware to penetrate the organization. They said the threat may have actually altered the footage recorded by the cameras, forcing the prison's representatives to catalog it as "tampered evidence."
Source: http://news.softpedia.com/news/Conficker-Worm-Compromises-Prison-CCTV-Systems-293505.shtml

34. *September 19, Salt Lake Tribune* – (Utah) **Cops in Utah, throughout Mountain West search for two jail escapees.** Local law enforcement agencies throughout Utah and the intermountain west were on the lookout September 19 for two escapees who broke out of eastern Utah's Uintah County Jail and stole an SUV. The inmates fled the Vernal jail through the vent of a laundry room where they worked, the undersheriff said. Law officers also were on alert in northern Utah and neighboring States. Gaining exit from the area was not simply a case of kicking out a vent, as initially reported. The vents, with 3-by-2-foot openings, had security screening in addition to a vent screen. "It took them a little work to get through those. We didn't think anyone could," the undersheriff said.
Source: http://www.sltrib.com/sltrib/news/54925542-78/escapees-jail-utah-foot.html.csp

35. *September 18, MLive.com* – (Michigan) **Ingham County 911 Center suffers two hour radio outage, service to residents not affected.** A technician's error caused the radio systems at the Ingham County, Michigan 9-1-1 center to go down for 2 hours September 18, an official with the center confirmed. The deputy controller said the center suffered a complete failure of its radio systems. The radio systems are utilized by dispatchers to communicate with emergency workers and public safety officers. Communications between dispatchers and officers, firefighters, and medical personnel were not disrupted, despite the failure; officials switched communications to the conventional backup system.

Source: http://www.mlive.com/lansing-news/index.ssf/2012/09/ingham_county_911_center_suffe.html

For another story, see item **46**

[Return to top]

Information Technology Sector

36. *September 20, The Register* – (International) **Hacktivists, blackhats snatch sixguns from whitehats' holsters.** Tools designed for testing server and network defenses are being used by hacktivists to launch denial-of-service (DoS) attacks on Web sites. More and more assaults are concentrating on exhausting Web apps and the HTTP server software running it, rather than simply flooding the underlying stack with bogus traffic to exhaust resources and bandwidth, according to the latest edition of Imperva's Hacker Intelligence report. This type of attack may be directed at specific types of Web servers such as IIS or Apache, or to specific applications, such as SharePoint. The latest and most popular distributed denial-of-service (DDoS) tools include LOIC, SlowHTTPTest, and railgun. The use of the latter two white-hat tools shows how black-hat hackers have begun running attacks that utilize white-hat testing tools. Attacks analyzed by Imperva in its report include network assaults by hacktivists in Bahrain, Colombia, and Russia, as well as Web blitzes against businesses linked to DDoS-for-hire scams. DDoS attacks typically run from botnet networks of compromised computers.
Source: http://www.theregister.co.uk/2012/09/20/ddos_trends_imperva/

37. *September 20, Homeland Security News Wire* – (International) **New NIST publication provides guidance for computer security risk assessments.** The National Institute of Standards and Technology (NIST) released a final version of its risk assessment guidelines which, NIST says, can provide senior leaders and executives with the information they need to understand and make decisions about their organization's current information security risks and information technology infrastructures. A NIST release notes that information technology risks include risk to the organization's operations (including, for example, missions and reputation), its critical assets such as data and physical property, and individuals who are part of or served by the organization. In some cases, these risks extend to the nation as a whole. Risk assessments are part of an organization's total risk management process.
Source: http://www.homelandsecuritynewswire.com/dr20120920-new-nist-publication-provides-guidance-for-computer-security-risk-assessments

38. *September 20, Computerworld* – (International) **Microsoft: Patch for critical IE zero-day bug coming Friday.** September 19, Microsoft released a stopgap defense that protects Internet Explorer (IE) against attacks until the company issues a patch September 21. The update will fix five flaws, including one revealed by a security researcher the weekend of September 15 that hackers have been exploiting to hijack Windows PCs and infect them with malware. The so-called "zero-day" vulnerability — meaning it was leveraged by attackers before Microsoft was aware of the bug, much

less able to patch it — has been analyzed and discussed by security experts with increasing intensity since September 17.
Source:
http://www.computerworld.com/s/article/9231478/Microsoft_Patch_for_critical_IE_zero_day_bug_coming_Friday

39. *September 20, The Register* – (International) **Sophos antivirus classifies its own update kit as malware.** There were problems for Sophos users September 19 after the business-focused antivirus firm Sophos released an update that classified itself and any other update utility as a virus. As a result, enterprise PCs running the application became confused, generating false positives reporting SSH/Updater-B malware. System administrators were bombarded with automated alerts by email about the bogus problem. The issue was resolved with a functional update, issued later September 19. For many, troubles continued because many endpoints and corporate networks hit by the false positive have been left with systems that can no longer update themselves properly because the required functionality has been consigned to quarantine.
Source: http://www.theregister.co.uk/2012/09/20/sophos_auto_immune_update_chaos/

40. *September 20, The Register* – (International) **Latest iPhone hacked to blab all your secrets.** Dutch hackers exploited a WebKit bug in mobile Web browser Safari to wipe an iPhone 4S of its photos, address book contacts, and its browser history. The flaw exists in Apple's iOS 5.1.1 and the latest developer preview of iOS 6, which was made public September 19. As such, the vulnerability should affect iPhones, iPads, and modern iPods — including the new iPhone 5. The vulnerability could also exist in BlackBerry and Android phones, which also use the WebKit engine in their built-in Web browsers, although the hack has not been tested on these platforms. The bug was demonstrated by the team at Certified Secure at the Pwn2Own Mobile hacking contest in Amsterdam, Netherlands, the week of September 17. A Samsung Galaxy S3 was also broken into and compromised by a separate team at MWR Labs using wireless near-field communication (NFC) technology.
Source: http://www.theregister.co.uk/2012/09/20/iphone_hack_photos_contacts_taken/

41. *September 20, Softpedia* – (International) **Over 1 million PCs currently part of ZeroAccess global botnet.** The piece of malware known as ZeroAccess is present on more than 1 million computers spread throughout almost 200 countries. So far, the threat was found to be installed more than 9 million times on the devices of unsuspecting users. The total number of installs reached this limit in just several months. ZeroAccess generates a profit for its masters with the aid of a peer-to-peer network that is used to download malicious plugins. These components are capable of carrying out diverse tasks that help the criminals make money. According to experts, cyber criminals can earn as much as $100,000 per day if the botnet is operating at maximum capacity. After monitoring the threat for 2 months, Sophos was able to pinpoint the locations of the infected machines. Most appear to be in the United States (55 percent), Canada, the United Kingdom, Germany, Turkey, Spain, France, Austria, Italy, and Japan.
Source: http://news.softpedia.com/news/Over-1-Million-PCs-Currently-Part-of-ZeroAccess-Global-Botnet-293573.shtml

42. *September 20, Softpedia* – (International) **Users of mobile portals exposed to HTTP header pollution attacks, expert finds.** At the EUSecWest security conference in Amsterdam, Netherlands, an independent security researcher unveiled his findings on GSM vulnerabilities in a paper entitled "Using HTTP headers pollution for mobile networks attacks." The attacks he demonstrated target the Wireless Application Protocol (WAP) and Web portals on which the customers of mobile operators can perform specific tasks such as money transfers, content downloads, and subscriptions. Depending on the services offered by the carrier on these Web sites, cyber criminals can abuse the security holes for their own gain. Apparently, there is also a way for shady companies to take advantage of these flaws. Third-party mobile content providers can enter agreements with the carrier and secretly subscribe customers to their paid services. A majority of the sites tested by the researcher — belonging to operators from all over the world — were found to be vulnerable to the attack method he identified.
    Source: http://news.softpedia.com/news/Users-of-Mobile-Portals-Exposed-to-HTTP-Header-Pollution-Attacks-Expert-Finds-293540.shtml

43. *September 20, The H* – (International) **Apple closes numerous security holes with iOS 6.** With the release of iOS 6.0, Apple not only delivers several new features to the mobile operating system but also closes many security vulnerabilities. The major update deals with a list of almost 200 CVE items, some of which apply to several vulnerabilities. The problems grant hackers almost free reign: They range from a hole that lets attackers circumvent the passcode on the lock screen, to the ability to fake text message sender information and code injection through specially prepared Web sites or media files. One vulnerability is caused by an error in the way the operating system parses some configuration files. The hole allows attackers to pretend an important system update is available for the user's device. This update appears to be signed by Apple or the user's mobile carrier, when in fact it is completely fake. If the user installs the so-called "update," the malicious configuration file is able to change critical system settings. Through this attack vector, hackers can configure a proxy on the system and are able to breach the encrypted data connections of the iOS device. This can even give hackers access to the Apple account of the victim, allowing them to spend the victim's money in the iTunes Store. This vulnerability was first publicly disclosed 3 years ago.
    Source: http://www.h-online.com/security/news/item/Apple-closes-numerous-security-holes-with-iOS-6-1713012.html

44. *September 19, Dark Reading* – (International) **Attack easily cracks Oracle database passwords.** A researcher with AppSec Inc. plans to show an attack exploiting cryptographic flaws he discovered in Oracle's database authentication protocol at the Ekoparty security conference in Buenas Aires, Argentina. It allows an attacker without any database credentials to brute-force hack the password hash of any database user so he/she then can access the data. The researcher and his team first reported the bugs to Oracle in May 2010. Oracle fixed them in mid-2011 via the 11.2.0.3 patch set, issuing a new version of the protocol. "But they never fixed the current version, so the current 11.1 and 11.2 versions are still vulnerable," the researcher said, and Oracle has no plans to fix the flaws for version 11.1.

Source: http://www.darkreading.com/authentication/167901072/security/application-security/240007643/

45. *September 18, V3.co.uk* – (International) **Flame malware siblings still running wild and undetected, warn researchers.** The week of September 17, Kasperksy claimed to have detected three Flame-related pieces of malware in the wild. Kaspersky's chief malware expert told V3.co.uk that analysis of the command and control (C&C) servers used by Flame's authors indicated the extent of the cyber espionage campaign may be larger than first thought. As such, he warned there are likely more than the three new Flame-level threats currently operating undetected in the wild.
Source: http://www.v3.co.uk/v3-uk/news/2206227/flame-malware-siblings-still-running-wild-and-undetected-warn-researchers

For more stories, see items **7**, **9**, **10**, **12**, **29**, **33**, and **46**

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

46. *September 19, Warminster Patch* – (Pennsylvania) **Verizon outage disrupts Bucks and Montgomery County.** Verizon's private and business FiOS customers in Bucks and Montgomery County, Pennsylvania, felt the effects of a September 18 storm well into September 19, spending most of the day without phone and Internet service. Verizon's media relations manager for the northeast region said the trouble started September 18 when a tree toppled over power lines outside the company's Hatboro office. The back-up generator maintained operations until it shut down September 19. When the generator regained power, it began recharging the office's bank of back-up batteries. One battery began to overheat, forcing technicians to shut down power again to repair the faulty equipment. The loss of FiOS service not only left residential customers without phone service for a bulk of the day, but also affected the 9-1-1 systems for Bucks and Montgomery counties. Local businesses that use FiOS for credit card transactions also experienced network connectivity issues.
Source: http://warminster.patch.com/articles/storm-damage-disrupts-verizon-service-in-bucks-and-montgomery

For more stories, see items **40**, **42**, and **43**

[Return to top]

Commercial Facilities Sector

47. *September 20, WBIR 10 Knoxville* – (Tennessee) **Gas leak evacuates several West Knox businesses.** Several West Knoxville, Tennessee, businesses were evacuated because of a gas leak September 19. The Knoxville Fire Department (KFD) stated that firefighters were dispatched to investigate the smell of natural gas at the scene. There was no one in the building, so firefighters forced their way into the business, American Printing, which is next door to Union Jacks pub. The building was full of gas, and KFD evacuated several nearby businesses for safety reasons. Firefighters stood by as Knoxville Utility Board workers dug into the ground to access the gas line feeding the building and clamped it shut. The building was then purged with fresh air.
Source: http://www.wbir.com/news/article/235294/2/Gas-leak-evacuates-several-West-Knox-businesses

48. *September 20, WLS 7 Chicago* – (Illinois) **3-month-old dies in West Side fire.** A fire in Chicago left 1 victim dead and 30 people out of their homes, WLS 7 Chicago reported September 20. The victim was found in a room after the fire broke. Firefighters said they believe the fire started in the room where the victim was found, but they do not know how it started. "Heavy fire damage on the first floor. The fire appears to have originated there. The back porches are off the back of the building. The fire did get into all four apartments, not heavily on the east side, but heavy enough on the west side," said a Chicago Fire Department spokesman. It was unclear whether smoke detectors worked in the apartment complex, but firefighters would be out in the neighborhood September 20 to hand out new smoke detectors to neighbors.
Source: http://abclocal.go.com/wls/story?section=news/local&id=8817604

49. *September 19, Press of Atlantic City* – (New Jersey) **Stove fire in Atlantic City forces evacuation of 40 people.** About 40 people were evacuated after a stove fire at the Inlet Towers in Atlantic City, New Jersey, September 19. Two individuals were in a third-floor apartment when the stove "exploded", the fire chief said. The two immediately vacated the apartment and left the door open, which spread smoke into the hallway. About 20 people on the third floor and 20 on the fourth had to be evacuated. Those out of their apartments were temporarily staying at Jefferies Towers, but were expected to be back home within a few hours, the fire chief said.
Source: http://www.pressofatlanticcity.com/communities/atlantic-city_pleasantville_brigantine/stove-fire-in-atlantic-city-forces-evacuation-of-people/article_68beee1a-028f-11e2-aab2-0019bb2963f4.html

50. *September 19, Contra Coasta Times* – (California) **Pre-dawn fire burns businesses in Montclair strip mall.** A two-alarm predawn fire September 19 eventually damaged or destroyed four businesses at a strip mall in Montclair, California. The fire spread from a market and a Mexican restaurant to a diet clinic and the Panamericana Travel Systems offices. The travel business occupied two units in the strip mall. Firefighters cut holes in the roof to prevent the fire from spreading to six additional units. They also attempted to fight the blaze from inside the structure, but eventually retreated because of concerns that the roof would collapse. The fire destroyed the market and restaurant. The other two businesses sustained damage from the blaze, but might be saved.

Source: http://www.contracostatimes.com/california/ci_21580781/montclair-strip-mall-damaged-fire

51. *September 19, Clifton Journal* – (New Jersey) **Chlorine spill evacuates Jewish Center in Clifton.** The Clifton Fire Department's HAZMAT unit was dispatched to the Jewish Family Service Children's Center in Clifton, New Jersey, September 19 after 75 gallons of chlorine leaked in a storage room near the Olympic-sized pool. The Clifton fire chief said a worker moving materials accidentally hit and broke off the chlorine valve, causing 75 gallons of sodium hypochlorite, a liquid, to spill on the floor. The fire department was alerted and the worker was transported to al hospital after complaining about burns on his hands, ankles and face. The fire chief explained that the concentration in the facility was relatively low at 12 percent and stated a higher concentration may cause serious bodily burns and injuries. As the HAZMAT unit took care of the leak, firefighters evacuated about 75 people from the building. After the Clifton Fire Department secured the scene, it was turned over to the center for cleanup with supervision by a Passaic County Health Department official.
Source: http://www.northjersey.com/news/170394876_Chlorine_spill_evacuates_Jewish_Center_in_Clifton.html

For another story, see item **1**

[Return to top]

National Monuments and Icons Sector

52. *September 20, KFYR 5 Bismarck* – (North Dakota) **Over 1,000 acres burned in Mandaree wildfire.** A wildfire has burned more than 1,000 acres near Mandaree, North Dakota, KFYR 5 Bismarck reported September 20. According to a Three Affiliated Tribes Fire Management officer, crews arrived September 19 to a wildfire created by warm temperatures and strong winds. As of September 20, the fire was 35 percent contained. No structures were burned.
Source: http://www.kfyrtv.com/News_Stories.asp?news=59368

[Return to top]

Dams Sector

53. *September 19, Santa Cruz Sentinel* – (California) **Flooding risk reduced along Pajaro River: Phase 1 of $8.3 million levee project complete.** The first phase of an $8.3 million flood protection project along the Pajaro River near Watonsville, California, was completed September 19. Since March 1995, Santa Cruz and Monterey counties worried about the risk of a major flood after a levee breach that caused floodwaters to ravage the town of Pajaro and more than 3,000 acres of Monterey County farmland. Damage totaled nearly $100 million. In the wake of the flood, the U.S. Army Corps of Engineers received federal support to rebuild a 12-mile stretch of levee. The idea was to provide 100-year flood protection but the project stalled amid disputes over plans

and federal funding shortfalls. The current project, known as bench excavation, was conceived in 2005 as an interim step, also taking far longer than expected as officials built consensus among stakeholders on a design, secured permits from regulatory agencies, and persuaded the State to provide $7.5 million in grants to help pay for the work. The first phase removed 140,000 cubic yards of sediment from the levee channel between Highway 1 and just east of the Main Street bridge connecting downtown Watsonville with Pajaro. The second phase, expected to begin in June 2013 and wrap up in October 2013, will dig out another 190,000 cubic yards between Salsipuedes Creek and Murphy Road.
Source: http://www.contracostatimes.com/california/ci_21587037/flooding-risk-reduced-along-pajaro-river-phase-1

[Return to top]

NTAS
National Terrorism Advisory System

NO ACTIVE ALERTS
www.DHS.gov/alerts

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

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.