Homeland Security

Daily Open Source Infrastructure Report 19 September 2012

Top Stories

- A FBI report shows cybercriminals targeted banks and credit unions, using spam, phishing emails, and malware, to illegally transfer money in amounts between $400,000 and $900,000. – *Softpedia* (See item **7**)
- Peregrine Financial Group's CEO pleaded guilty in court in Iowa to carrying out a 20-year fraud that stole $200 million from about 24,000 customers. – *Associated Press* (See item **9**)
- Al Qa'ida's branch in North Africa is calling for attacks on U.S. diplomats in many countries, and an escalation of protests against an anti-Islam video that triggered a wave of demonstrations. – *Associated Press* (See item **25**)
- Students at Louisiana State University returned to their dorms September 17, many hours after a bomb threat. Police spoke to counterparts in other States hit during a recent spate of bomb threats against colleges. – *Reuters* (See item **29**)
- Microsoft issued a security advisory September 17 that confirmed in-the-wild attacks are exploiting an unpatched bug in Internet Explorer (IE), which comprises 53 percent of all browsers used worldwide. – *Computerworld* (See item **39**)
- Firefighters continued to battle wildfires in Washington that scorched dozens of square miles of acreage, burned or threatened thousands of structures, and forced hundreds of evacuations. – *Associated Press; Yakima Herald-Republic* (See item **48**)

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 18, WNYF 7 Watertown* – (New York) **Route 68 re-opens following tanker spill.** A section of State Route 68 in Canton, New York, where crews worked to contain a fuel spill, was re-opened to motorists September 18. A fuel truck overturned the afternoon of September 17 near the intersection with County Route 14. State Department of Environmental Conservation (DEC) officials said the initial cleanup wrapped up around 8 p.m. and the truck was removed. Roughly 2,200 gallons of fuel either leaked or remained in the tank that ruptured, a DEC spokesman said. About 150 tons of contaminated soil was removed. About another 2,000 tons of soil with less contamination still must be removed, which should be completed over the next few weeks. About 7,300 gallons of fuel was not affected by the crash and was recovered.
   Source: http://www.wwnytv.com/news/local/Canton-Tanker-Rolls-Over-Leaking-Fuel-170047586.html?skipthumb=Y

2. *September 18, San Francisco Business Times* – (International) **Chevron fined $17.3 million for Brazil oil spill.** Brazil's National Petroleum Agency has fined Chevron Corp. $17.3 million for its role in an offshore oil spill in 2011, the Wall Street Journal reports, according to the San Francisco Business Times, September 18. The fine covers 24 of 25 sanctions that the agency issued Chevron earlier this year, and could be increased when a decision is made on the final sanction. An estimated 3,700 barrels of oil leaked into the ocean from the Frade field last November, and Brazil charged several Chevron executives with various crimes, including altering documents and breaches of regulations. Chevron and the drilling company Transocean Ltd. are also facing civil and criminal lawsuits related to the spill.
   Source: http://www.bizjournals.com/sanfrancisco/morning_call/2012/09/chevron-fined-173m-for-brazil-oil.html

[Return to top]

Chemical Industry Sector

3. *September 17, WSBT 22 South Bend* – (Indiana) **Report: EPA responsible for chemical leak.** The U.S. Environmental Protection Agency (EPA) said its own mistake caused a chemical fire and leak at an abandoned Mishawaka, Indiana factory. An EPA incident report said contractors working to clean up the old Baycote building left two different chemicals — cyanide and sodium hydrosulfite — too close together, causing them to spontaneously combust. The fire and leak led to an evacuation of about 200 people September 14. Sodium hydrosulfite is a highly reactive chemical, the report says, and the combination is likely what caused the fire to ignite, but the official cause of the fire is still under investigation. Clean up continued September 17 inside the building that Mishawaka's mayor said has had many problems. "The building was literally corroding from within," he said. "The roof was collapsing, beams were corroding, tanks were corroding." The EPA's on-scene coordinator said some materials were mismarked and difficult to identify when contractors started clean up earlier this year. He said mistakes like the one EPA contractors made by accidentally putting chemicals too close together are rare. The plan is to have clean up finished by November, the on-scene coordinator added.
Source: http://articles.wsbt.com/2012-09-17/atkociunas_33907538

4. *September 17, Milwaukee-Wisconsin Journal Sentinel* – (Wisconsin) **EPA tallies nearly 9,000 gallons of hazardous material at abandoned factory.** Federal emergency response contractors have inventoried 8,868 gallons of hazardous chemicals inside an abandoned metal plating factory in Slinger, Wisconsin, a U.S. Environmental Protection Agency (EPA) official said September 17. The chemicals were found stored in 315 barrels, drums, vats and large jugs at the former Niphos Coatings company, said an on-scene coordinator with the EPA's Superfund program in Chicago. An additional 100 jars and other small containers of laboratory chemicals are in the building, he said. September 17, contractors continued physically separating containers of various chemicals for removal and disposal. Two chemicals inside are considered extremely hazardous: nitric acid and sodium cyanide. Niphos closed in March 2010. The owner has not paid property taxes since 2007, and has not filed chemical inventory reports required under federal law since 2008, records show.
Source: http://www.jsonline.com/news/ozwash/epa-tallies-nearly-9000-gallons-of-hazardous-material-at-abandoned-factory-a76sv55-170052356.html

5. *September 17, KSLA 12 Shreveport* – (Louisiana) **Train cars carrying hazardous chemicals derail in Claiborne Parish.** Five rail cars containing hazardous materials went off track September 17 in Claiborne Parish, Louisiana, but no chemical leaks have been found. Still, authorities cordoned off a 1-mile radius surrounding the train derailment as a precaution. Claiborne Parish sheriff's officials said the nearest residence is about 2 miles from the derailment. The derailed cars contained five chemicals: chlorine, sulphur, benzine, methyl, and alkamide. The sheriff's department dispatched hazardous materials technicians to the scene. The next concern is moving the cars as Louisiana & North West Railroad officials must keep the tanks from leaking when they are picked up and put back on the track.

Source: http://www.ksla.com/story/19567310/train-cars-carrying-hazardous-chemicals-derail-in-claiborne-parish

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

6. *September 18, Associated Press* – (National) **Feds expand Hyundai Elantra air bag probe after severed ear claim.** The National Highway Traffic Safety Administration added the 2011 and 2013 model years to an investigation of an air bag problem with 2012 Hyundai Elantras that cut a car owner's ear in half, the Associated Press reported September 17. The agency also upgraded the probe to an engineering analysis, a step closer to a recall. The agency started investigating 123,000 2012 Elantras in May, but now said only Korean-built Elantras have the part that caused the problem. About 75,000 were sold in the U.S. In April, an Elantra owner told investigators a side air bag inflated in a crash and a metal bracket sliced the driver's ear. Hyundai said the problem appears to be isolated.
   Source: http://www.freep.com/article/20120917/BUSINESS01/120917049/Feds-expand-Hyundai-Elantra-air-bag-probe

For more stories, see items **4** and **13**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

7. *September 18, Softpedia* – (International) **FBI: Networks of financial institutions targeted with malware, RATs, and keyloggers.** A FBI report shows that cybercriminals have started focusing their efforts on targeting the networks of financial institutions, Softpedia reported September 18. Cybercriminals are relying on spam, keyloggers, Remote Access Trojans (RATs), phishing, and other malicious elements to steal employee log-in credentials. The Internet Crime Complaint Center (IC3) reported that the stolen information has been utilized to perform unauthorized wire transfers for amounts between $400,000 and $900,000. In the first phase of these operations, the criminals use spam and phishing emails. Once they compromise the machine of an

employee, they plant RATs, keyloggers, and other pieces of malware to gain access to internal networks and the details needed to access third party systems. Most of the victims appear to be small to medium-sized banks and credit unions, but major financial institutions have also been targeted. In some cases, the crooks launched distributed denial-of-service attacks against the bank's Web site, most likely to cover up their fraudulent transactions.
Source: http://news.softpedia.com/news/FBI-Networks-of-Financial-Institutions-Targeted-with-Malware-RATs-and-Keyloggers-293126.shtml

8. *September 18, The Register* – (International) **'How I crashed my bank, stole PINs with a touch-tone phone'.** Miscreants can crash or infiltrate banks and help desks' touch-tone and voice-controlled phone systems with a single call, a security researcher warned, according to The Register September 18. A researcher who works for iSight Partners said audio processing algorithms in office telephone networks and speech-driven command software are liable to crash when bombarded with unusual data in "fuzzing" attacks. Certain DTMF (Dual-Tone Multi-Frequency) signals can cause private branch exchanges (PBX) and interactive voice response (IVR) systems to raise exceptions and bail out, much in the same way unexpected input data can disrupt applications running on a desktop computer or server. PBX and IVR machines are often used to run phone banking, call centers, and other interactive telephone systems. Given the appropriate DTMF input, it may be possible to crash backend application servers or convince them to cough up sensitive data. Repeating the trick to bring down a machine effectively launches a denial-of-service attack on the phone line as a paper by the researcher explained. "We would be able to extract sensitive information about the application's hosted environment with these sorts of bugs. Since applications that use DTMF algorithms are mainly phone-based, it was possible to extract output in the form of audio data", he said. He also claimed it was possible to extract customer PINs from an unnamed Indian bank.
Source: http://www.theregister.co.uk/2012/09/18/dtmf_phone_system_hack_attack/

9. *September 18, Associated Press* – (Iowa; National) **Peregrine CEO pleads guilty in scandal.** Peregrine Financial Group's CEO pleaded guilty in court in Iowa, September 17 to carrying out a 20-year, $200 million fraud that he first confessed to in a note found on him after an unsuccessful suicide attempt in July. The CEO pleaded guilty to charges of mail fraud, embezzling customer funds, and making false statements to two regulatory agencies. He acknowledged that he secretly withdrew funds from about 24,000 customers starting in the 1990s, and used computers to make phony bank statements to conceal the theft. He gave fraudulent statements to his accounting department showing fictitious deposits and balances. The false numbers were used to generate monthly reports to regulators showing the company was holding more than $200 million in customer funds than it actually had. He fooled auditors with the National Futures Association by changing the bank's address in the statements to a post office box he controlled. The auditors would mail forms asking the bank to verify Pergrine's account balances; the CEO would send back false documents purporting to be from the bank.
Source: http://www.omaha.com/article/20120918/MONEY/709189965/1707

10. *September 18, The Register* – (International) **Romanians plead guilty to credit card hack on U.S. Subway shops.** Two Romanian nationals who were extradited to the United States in May confessed their involvement in a $10 million scam aimed at stealing credit and debit card data from payment terminals at hundreds of Subway restaurants and other merchants across the country, according to a U. S. attorney's office, The Register reported September 18. They were among four Romanian nationals extradited in May after being charged in December 2011 with hacking into Subway vulnerable point-of-sale (POS) computers between 2009 and 2011. The scheme led to the compromise of more than 146,000 payment cards. The hack against POS terminals relied on identifying machines running exploitable remote desktop software applications. The U.S. Department of Justice said one of the men hacked into these systems to install keystroke logging applications, which subsequently recorded card data from swiped cards before transferring this information to dump sites. In some cases he had to crack passwords to circumvent the remote desktop applications, which in normal use were used to update the software on POS terminals. The other individual admitted to attempting to make fraudulent transactions using the stolen credit card data as well as selling the data to co-conspirators.
Source: http://www.theregister.co.uk/2012/09/18/romanian_cybercrooks_plead_guilty/

[Return to top]

Transportation Sector

11. *September 18, Associated Press* – (New York) **Stun gun pen found in luggage at JFK.** Authorities said a man was arrested at New York's John F. Kennedy International Airport security checkpoint after a stun gun pen was discovered in his luggage September 17. The Transportation Security Administration contacted the Port Authority police, who arrested the passenger on a State weapons charge and confiscated the stun gun. Airport operations were not affected.
Source: http://www.cbs6albany.com/template/inews_wire/wires.regional.ny/224a04ba-www.cbs6albany.com.shtml

12. *September 18, New York Post* – (New York; Texas) **JFK hijack scare.** Three packed passenger jets were searched at New York City's John F. Kennedy International Airport September 17 after an anonymous phone caller claimed there were Islamic hijackers aboard armed with explosives — but it was nothing but a hoax, law-enforcement sources said. The jets, American Airlines flights 24 and 846, and Finnair Flight 5, were instructed to park in a remote part of the airport for security inspections after they landed on schedule. Police gave them a 90-minute once-over before declaring the call a hoax. Two other U.S. airports, including one in San Antonio, received similar fake calls, the sources said. The caller, who spoke to Kennedy's Port Authority police desk, said he got the information from a member of an unnamed Muslim terrorist group. He claimed that the hijackers were hiding in the wheel wells of the plane and were wearing gas masks, one law-enforcement source said. The pilots reported no indications that anything was wrong.
Source:

http://www.nypost.com/p/news/local/jfk_hijack_scare_1E9Nq6ujbaI0XUncKAu6HL?utm_medium=rss&utm_content=Local

13. *September 18, National Transportation Safety Board* – (National) **NTSB issues 2 urgent safety recommendations to FAA.** The National Transportation Safety Board (NTSB) September 18 issued two urgent safety recommendations to the Federal Aviation Administration (FAA) regarding two recent occurrences in which the fan midshaft on General Electric GEnx-1B engines fractured or exhibited crack indications; and a GEnx -2B incident that appears similar in nature. The recommendations are: (1) Issue an airworthiness directive to require, before further flight, the immediate ultrasonic inspection of the fan midshaft in all GEnx-1B and -2B engines that have not undergone inspection, and (2) Require repetitive inspections of the fan midshaft at a sufficiently short interval that would permit multiple inspections and detection of a crack before it could reach critical length and the fan midshaft fractures. July 28 the NTSB initiated an investigation of an engine failure that occurred on a Boeing 787 during a pre-delivery taxi test in Charleston, South Carolina. This investigation is ongoing. In addition, August 31, a GEnx-1B engine installed on a Boeing 787 that had not yet flown was found to have an indication of a similar crack on the fan midshaft. The fan midshaft was removed from the engine for further inspection and examination. As a result of the investigative work to date, the NTSB has determined that the fan midshafts on the GEnx engines fractured or cracked at the forward end of the shaft where the retaining nut is installed.
Source: http://news.thomasnet.com/companystory/NTSB-Issues-2-Urgent-Safety-Recommendations-to-FAA-621970

14. *September 17, Associated Press* – (Wisconsin) **Delta flight returns to Green Bay after smoke fills cockpit.** Officials from Green Bay, Wisconsin's Austin Straubel International Airport said a Delta flight made an emergency landing after smoke filled the airplane's cabin, the Associated Press reported September 17. An airport director said the Detroit-bound flight left Green Bay September 16. He said the plane's cabin filled with smoke, forcing it to return to Austin Straubel where it made an emergency landing about a half-hour later. Sixty-five passengers and a crew of four evacuated on the taxiway using a set of stairs. They were taken to the terminal where a medical crew checked everyone. No one was transported to the hospital. WLUK 11 Green Bay reported officials have not said what caused the smoke.
Source: http://travel.usatoday.com/flights/story/2012/09/17/delta-flight-returns-to-green-bay-after-smoke-fills-cockpit/57794040/1

For more stories, see items **1**, **5**, and **24**

[Return to top]

Postal and Shipping Sector

15. *September 17, Aberdeen Patch* – (Maryland) **Devices detonate mailbox, burn car near Aberdeen.** The Maryland State Fire Marshal's office was investigating incidents that led to a car blaze and an explosion in a mailbox September 16 outside of Aberdeen,

Maryland; the incidents took place in a 90-minute span in the Perryman community. The Aberdeen Fire Department responded after an explosive detonated in a custom steel mailbox. Around 90 minutes earlier, the Aberdeen Fire Department and Harford County Sheriff's Office responded to a vehicle fire. A Yukon Denali XL was found "totally consumed by fire in a field" in the rear of an industrial park, authorities said. The fire marshal said the blaze was caused by an incendiary device in the interior of the vehicle.
Source: http://aberdeen.patch.com/articles/devices-detonate-mailbox-burn-car-in-perryman-sept-17-2012

For another story, see item **27**

[Return to top]

Agriculture and Food Sector

16. *September 18, Food Safety News* – (International) **Ground beef recalled for E. coli risk across Canada.** Ground beef products sold at major grocery chains across Canada were recalled because they may be contaminated with E. coli. The Canadian Food Safety and Inspection Agency (CFIA) announced September 17 that XL Foods of Alberta was recalling various ground beef products such as patties, meatballs, and meatloaf because the ground beef from which they were made may contain E. coli. The majority of the affected foods were sold to retail stores in Alberta, British Columbia, Saskatchewan, Manitoba, and Ontario, but Costco's Kirkland Signature brand was sold at stores nationwide. Other companies who carry the affected meats include Safeway, Walmart, and Calalhoo Meats. Products subject to the recall include ground beef, burger patties, ground chuck, ground sirloin patties, stuffed peppers, meatballs, beef sliders, meatloaf, cheddar cheese patties and ground beef tubes. CFIA said that the recall is part of an ongoing food safety investigation and that it is working to verify all involved products and determine whether any more may need to be recalled.
Source: http://www.foodsafetynews.com/2012/09/ground-beef-sold-across-canada-recalled-for-e-coli-risk/#.UFhp7K66TlY

17. *September 18, Associated Press* – (North Dakota) **ND stiffens rules for female cattle imports.** North Dakota stiffened cattle import rules because of cases of a bovine venereal disease in other States, the Associated Press reported September 18. The State veterinarian said the board of animal health recently voted to tighten the restrictions for female cattle imports because of concerns about trichomoniasis, which can cause infertility and miscarriages in cattle. She said officials expect more cattle to be brought into North Dakota because of drought in other States.
Source: http://www.necn.com/09/18/12/ND-stiffens-rules-for-female-cattle-impo/landing_nation.html?&apID=b6906ccb2686452cacb683a2a1be0109

18. *September 18, Associated Press* – (Idaho) **Fire causes $2 million in damages to hop shed.** Fire officials in Wilder, Idaho, were investigating the cause of a fire that destroyed an estimated $2 million worth of hops and machinery used to dry the pine-cone like flowers. The fire September 16 ignited in one of several hop driers in a barn

outside the southwest Idaho city. The Wilder fire chief said the fire spread quickly and forced firefighters to focus on keeping the flames from spreading to other structures. Hops grow all across southwestern Idaho and are a key ingredient in the brewing of beer, lending bitterness and aromatic qualities.
Source: http://www.sacbee.com/2012/09/18/4830039/fire-causes-2-million-in-damages.html

19. *September 17, U.S. Food and Drug Administration* – (Oregon; Washington) **Peterson Company recalls Ricotta Salata Frescolina brand cheese for possible health risk in 2 States.** Peterson Company recalled Ricotta Salata Frescolina brand cheese that came from its supplier Forever Cheese of Long Island City, New York, the U.S. Food and Drug Administration reported September 17. Forever Cheese recalled this cheese product due to possible Listeria monocytogenes contamination. The cheese was sold to distributors, retailers, and restaurants in Washington and Oregon from July 17-September 10. The potential for contamination was noted after an illness was reported in connection with eating the cheese. Each and every distributor, retailer, and restaurant has been contacted in an effort to recall any and all remaining product in the marketplace.
Source: http://www.fda.gov/Safety/Recalls/ucm319734.htm

20. *September 17, Food Safety News* – (New York) **Ruling: Spice Co. linked to Salmonella outbreak owes $33 million.** A New York-based spice company whose pepper was pinpointed as the source of a 2009-2010 Salmonella outbreak owes $33 million to the salami maker that had to recall 1.4 million pounds of meat products because they were made with the contaminated spices, ruled a judge September 17. In March 2010, salami and other ready-to-eat meats produced by Rhode Island-based Daniele International, Inc. were linked to an outbreak of Salmonella Montevideo that sickened 272 people in 14 States. The company was obligated to recall the implicated products, which turned out to have been contaminated by red and black pepper — manufactured by Brooklyn, New York-based Wholesome Spice, Inc. — that was used to coat some of its meat products. Daniele filed a suit against Wholesome Spice in April 2010, but the spice company never responded. Wholesome Spice dissolved in April, according to the Wall Street Journal. Due to Wholesome's failure to respond to the suit, a district court judge granted Daniele's request for a default judgment, requiring the spice company to pay Daniele $33 million in damages, reported the Wall Street Journal. However, because Wholesome is no longer in operation, Daniele may not receive the payment it is owed, said a lawyer for the meat company.
Source: http://www.foodsafetynews.com/2012/09/ruling-spice-maker-responsible-for-salmonella-outbreak-owes-33-million/#.UFhp8a66TlY

21. *September 17, U.S. Department of Labor* – (Mississippi) **U.S. Department of Labor's OSHA cites Omega Protein for 25 safety and health violations following worker fatality at Moss Point, Miss., plant.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) September 17 cited Omega Protein Inc. with 25 safety and health violations based on an April inspection of the company's processing plant in Moss Point, Mississippi. OSHA initiated the inspection after the death of a worker who had been caught in a rotating screw conveyor. Twenty-one

serious violations involved failing to: have employees affix personal lockout devices to a group lockout device, develop a written respirator protection program, develop and document procedures for controlling hazardous energy, provide training for forklift operators, conduct annual noise training, properly secure compressed gas cylinders, and provide a suitable facility for quick eye and body drenching or flushing. OSHA also identified fall and electrical hazards; a lack of equipment guarding on rotating drums; fan blades and horizontal rotating shafts; and a lack of guarding on the belts and pulleys of the grinding screw and the hopper screw conveyor. Four other-than-serious violations were also cited. Proposed penalties totaled $79,200.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22992

[Return to top]

Water Sector

22. *September 18, Poughkeepsie Journal* – (New York) **A cleanup plan for Shenandoah.** Cleanup of the Shenandoah Superfund site in Hopewell Junction, New York would rely on a combination of natural processes and removal of chemicals from the spill point under a plan proposed by the U.S. Environmental Protection Agency (EPA), the Poughkeepsie Journal reported September 18. Efforts to deal with the spill have been under way since 2000, when it was discovered that solvents and metals dumped into a septic tank and a ground pit at the site of an IBM contractor contaminated the groundwater with tetrachloroethene, or PCE. The 140-home site was added to the Superfund list in 2001. Residents were connected to a public water supply system in 2009. The EPA's preferred cleanup plan calls for continued operation of a process at the spill site that draws contaminated groundwater out of the bedrock, removes the contamination, and releases treated water to a storm sewer system. That process went online in 2012 and would continue for 15 years. The public has until September 28 to comment on the plan. The balance of the cleanup plan would allow naturally occurring processes to filter out the remaining levels of PCE from the area affected by the spill, expected to take 30 years. The EPA preferred plan is expected to cost $4 million.
Source:
http://www.poughkeepsiejournal.com/article/20120918/NEWS04/309180016/A-cleanup-plan-Shenandoah?odyssey=mod|newswell|text||s&nclick_check=1

23. *September 16, Abilene Reporter-News* – (Texas) **Water boil notice issued for city of Anson water customers.** Water customers in Anson, Texas, were under a boil order September 16 due to consumption safety issues in the water system. The water plant supervisor said he noticed a blockage in the water line and believed a chemical solidified causing the stoppage. Bacterial samples were submitted September 16 to the Abilene office of the Texas Commission on Environmental Quality. The boil notice was expected to be lifted by September 19.
Source: http://www.reporternews.com/news/2012/sep/16/just-water-boil-notice-issued-anson/

24. *September 16, Zanesville Times Recorder* – (Ohio) **Dry weather, leak near Riverside likely cause of rash of line breaks.** Nearly 80 water line breaks in the past 2 months across Zanesville, Ohio, were likely caused by shifting ground, city officials said. Another likely contributor to brown water was a leak discovered the week of September 10 on a hydrant branch, the Zaneville Reporter said September 16. The lack of rain from early July through the end of August caused drought conditions throughout the region. Compacted ground around the pipes can give way and cause water line breaks, a service director said. The age of the water lines has been a concern for years, but the dry weather exacerbated the problem, he said. With inventory of hydrants and valves in good shape, the biggest expense for the city is repairing damaged roads.
Source:
http://www.zanesvilletimesrecorder.com/article/20120916/NEWS01/209160301

For another story, see item **30**

[Return to top]

Public Health and Healthcare Sector

Nothing to report

[Return to top]

Government Facilities Sector

25. *September 18, Associated Press* – (International) **Al Qaeda branch in North Africa calls for attacks on US diplomats.** Al Qa'ida's branch in North Africa is calling for attacks on U.S. diplomats and an escalation of protests against an anti-Islam video that triggered a wave of demonstrations in Muslim countries. In a statement released September 18, al Qa'ida in the Land of the Islamic Maghreb praised the killing of the U.S. ambassador to Libya, in an attack on the U.S. consulate in Benghazi September 11. The group threatened attacks in Algeria, Tunisia, Morocco, and Mauritania in response to the movie that denigrates the Prophet Muhammad. Yemen-based al Qa'ida in the Arabian Peninsula recently issued a similar call for attacks on U.S. diplomatic facilities. The group is al Qa'ida's most active branch in the Middle East.
Source: http://www.foxnews.com/world/2012/09/18/al-qaeda-branch-in-north-africa-calls-for-attacks-on-us-diplomats/

26. *September 18, Associated Press* – (Utah) **Police: Man took hostage in office building.** Police are investigating why a knife-wielding man took a worker hostage in the elevator of a downtown Salt Lake City building that houses FBI offices September 17. Salt Lake City police say the man was moving from floor to floor in the building and holding a man against his will at knife-point. He was detained by agents as he stepped off the elevator into the lobby of the FBI offices on the 12th floor. The victim, who works in the building, was unharmed. The Salt Lake Tribune reports the man did not resist arrest and was booked on suspicion of aggravated kidnapping. KTVX 4 Salt Lake City reports police have not determined a motive for the hostage taking or

whether it was targeted to the FBI.
Source: http://www.sfgate.com/news/article/Police-Man-took-hostage-in-office-building-3874064.php

27. *September 17, Tampa Bay Times* – (Florida) **Suspicious package prompts investigation at Pinellas courthouse.** Authorities were called September 17 to the Pinellas County, Florida Courthouse after the discovery of a suspicious package that contained a dirty white powder and a letter containing death threats. Initial tests showed nothing toxic in the powder, but it was taken to the University of South Florida for additional testing, said the manager of criminal court records for the Pinellas County Clerk's Office. The powder resembled concrete dust, she said. The letter had a return address from a Florida prison, she added. Hazardous materials crews from Pinellas Park and Largo fire departments responded to the criminal complex after someone on the second floor received the envelope, a sheriff's spokeswoman said.
Source: http://www.tampabay.com/news/publicsafety/suspicious-package-prompts-investigation-at-pinellas-courthouse/1252030

28. *September 17, Associated Press* – (California) **CA man arrested after blog post about killing kids.** A statement issued September 18 by the Los Angeles County sheriff says a man with guns in his Valencia, California home that overlooks two schools wrote an Internet post saying he was watching kids and would not mind murdering them. He was arrested on suspicion of making terrorist threats. The statement said Bristol, Connecticut police alerted sheriff's investigators to the blog, where an anonymous man said he wanted to kill kids like July's shootings in a movie theater in Aurora, Colorado. Investigators linked the posting to the man's home, where several firearms were found. Sheriff's officials are working with Bristol police and Yale University police.
Source: http://www.sfgate.com/news/article/CA-man-arrested-after-blog-post-about-killing-kids-3872900.php

29. *September 17, Reuters* – (Louisiana) **Students return to Louisiana State University after bomb scare.** Students at Louisiana State University (LSU) in New Orleans were allowed to return to their dorms late September 17 after police swept residential halls on the campus following a bomb threat. Dining and recreational facilities also were reopened, LSU said in a statement. The university was evacuated following a telephoned threat to the East Baton Rouge Parish emergency center at 10:32 a.m. and the center relayed the information to campus police, said a university spokesman. The university chancellor made the decision to evacuate the campus, and LSU alerted students, faculty, and staff via text message at about 11:30 a.m., he said. As word of the threat spread, public school officials placed three nearby elementary schools and one high school on lockdown, according to the East Baton Rouge Parish School System. Louisiana State Police were talking to their counterparts in other areas of the nation where university bomb threats were reported the week of September 10 of to determine whether there were similarities.
Source: http://www.reuters.com/article/2012/09/18/us-usa-louisiana-evacuation-idUSBRE88G15820120918?feedType=RSS&feedName=domesticNews

30. *September 17, WCMH 4 Columbus* – (Ohio) **Park-Stradley Hall remains evacuated after Ohio State water main break.** More than 1,000 students at Ohio State University in Columbus, Ohio, remained unable to stay in their residence halls after being evacuated September 16 due to an underground water main break. An Ohio State spokesman said the underground break was found under College Avenue between Drinko Hall and Smith Hall. The water main break prompted officials to shut off water to Park-Stradley and Baker halls, along with the Ohio Union. Water was restored September 17 and students were able to return to the Ohio Union and Baker Hall. However, 1,100 students at Park-Stradley Hall remained evacuated. The university's office of student life arranged alternative housing options for Park-Stradley residents. To date, 40 students requested alternative housing accommodations. According to the university, there is 10-12 feet of water in the basement of Park-Stradley Hall, which soaked electrical equipment. While water service was restored to all of the affected facilities, possible water damage in the mechanical rooms may delay the return of students to Park-Stradley Hall for at least another day.
   Source: http://www2.nbc4i.com/news/2012/sep/16/17/water-line-break-sends-2000-osu-students-out-dorms-ar-1173611/

31. *September 16, Associated Press* – (International) **French police reinforce security around US Embassy.** Police said they are reinforcing security around the American Embassy in Paris, France, after hundreds of people gathered outside the building September 15 to protest a film produced in the United States that insults the Prophet Muhammad. A police officer said more uniformed and plain clothes police were put in place September 16 on the streets surrounding the embassy. He said that 150 people were detained September 15 and had their ID's checked because the protest was unauthorized. One person remained in custody for roughing up an officer. The demonstration was part of a wave of protests outside U.S. diplomatic posts around the world, some of which have turned violent.
   Source: http://www.cbsnews.com/8301-501714_162-57513733/french-police-reinforce-security-around-us-embassy/

For another story, see item **43**

[Return to top]

Emergency Services Sector

32. *September 18, WSPA 7 Spartanburg* – (South Carolina) **Officers looking for guns stolen from Greenwood police cruiser.** A Greenwood, South Carolina police cruiser was broken into September 16 and several guns were stolen. According to a police report, an unmarked car, belonging to the department's narcotics unit, was the vehicle that was broken into. The report said the doors were left unlocked. A pistol, a shotgun, a bulletproof vest, 2,000 rounds of ammunition, several magazines for the pistol, and a black patrol bag were stolen from the car. The Greenwood police chief said that if the investigation showed the car was unlocked, then such a slip is a violation of the department's rules. He said the officer may face consequences as a result.

Source: http://www.independentmail.com/news/2012/sep/18/officers-looking-guns-stolen-greenwood-police-crui/

33. *September 18, Cincinnati Enquirer* – (Ohio) **CPD changes Taser policy after study finds they can cause death.** In light of a recently released scientific study that shows the electronic Taser stun guns can cause cardiac arrest and death, leaders of the Cincinnati Police Department — greater Cincinnati and northern Kentucky's largest police force — announced changes September 18 to the department's use of force policy regarding the devices. Earlier in 2012, the police chief said the findings concerned him so he felt a review of the city's Taser policy was prudent. The new rules prohibit front shots except in situations of self defense or defense of another. And, they direct officers never to aim the Taser X26 at a person's head, neck, eyes, throat, chest/breast, or genitals. Cincinnati's approximately 1,000 sworn officers began training on the new policy in September.
Source: http://news.cincinnati.com/article/20120918/NEWS/309180103/CPD-changes-Taser-policy

34. *September 17, Daytona Beach News-Journal* – (Florida) **Security guard faces charges of reporting fake incidents.** A security guard faces possible charges for calling 9-1-1 to report fake incidents that summoned a helicopter and police dogs to search for fictitious persons, a Volusia County, Florida sheriff's spokesman said September 17. Deputies are in the process of filing a charging affidavit with the State attorney's office to determine what the security guard will be charged with, said a sheriff's spokesman. The complaint stemmed from several incidents that the guard reported while working as a security guard at Manheim Auto Auction.
Source: http://www.news-journalonline.com/article/20120917/NEWS/309179968?Title=Security-guard-faces-charges-of-reporting-fake-incidents

35. *September 17, National Journal* – (Florida; National) **Undercover cops use smartphones to monitor protests.** A network that allowed undercover police to use smartphones and tablets to monitor and communicate during protests at the Republican National Convention has given new meaning to having "eyes on the ground," National Journal reported September 17. At the 2012 Republican National Convention in Tampa, Florida, police tried out a new tool that can turn officers' smartphones into multimedia surveillance and communication platforms. In Tampa, emergency responders used specialized apps and software to turn off-the-shelf smartphones and tablets into tools for sending real-time video, voice, and data. That allowed undercover officers to transmit real-time video, for example, of protesters as they moved about the streets. The network in Tampa was used with special permission from the Federal Communications Commission. It was part of an effort to eventually develop a similar $7 billion National Public Safety Broadband Network for everyday use across the country. In addition to law-enforcement surveillance and communication, a future network could allow firefighters to transmit building plans to each other, or allow paramedics to review multimedia health records.
Source: http://mashable.com/2012/09/17/smartphones-monitor-protests/

36. *September 17, WCMH Columbus 4* – (Ohio) **Licking County 911 center experiencing an outage.** The 9-1-1 center for Licking County, Ohio, said the center was experiencing an outage for portions of the county, WCMH 4 Columbus reported September 17. The Licking County 9-1-1 center reported that the 828 Exchange was down, which affected residents in Harrington, Fallsburg, and Frazeysburg.
Source: http://www2.nbc4i.com/news/2012/sep/17/licking-county-911-center-experiencing-outage-ar-1174302/

37. *September 17, Park Rapids Enterprise* – (Minnesota) **Fiber optic cut affects regional use of 911 from cell phones.** An accidental fiber cut in the area has knocked out 9-1-1 service to most cell phone users, the Park Rapids Enterprise reported September 17. According to a news release from the Beltrami County, Minnesota Sheriff's Office, the fiber cut impacts cell phone users with AT&T, Verizon, and Northern PCS. Those who dial 9-1-1 will receive a busy signal. Crews are working to repair the damage.
Source: http://www.parkrapidsenterprise.com/event/article/id/34158/group/homepage/

38. *September 17, Redlands-Loma Linda Patch* – (California) **Sixteen fire hydrants stolen in northwest Redlands, estimate $40,000 to replace.** The city of Redlands, California, September 17 announced the theft of 16 fire hydrants in northwest Redlands. The estimated cost of replacing the missing hydrants is $40,000, according to Redlands Municipal Utilities and Engineering Department staff. The thefts occurred between September 11-12.
Source: http://redlands.patch.com/articles/sixteen-fire-hydrants-stolen-in-northwest-redlands-est-40-000-to-replace

[Return to top]

Information Technology Sector

39. *September 18, Computerworld* – (International) **Microsoft confirms hackers exploiting critical IE bug, promises patch.** September 17, Microsoft issued a security advisory that confirmed in-the-wild attacks are exploiting an unpatched bug in Internet Explorer (IE). The software maker is working on a fix. The advisory addressed the zero-day vulnerability that was found and disclosed by a researcher the weekend of September 15. September 17, the Metasploit open-source penetration framework published an exploit module for the bug. All but one supported edition of IE are affected: 2001's IE6, 2006's IE7, 2009's IE8, and 2011's IE9. Together, those browsers accounted for 53 percent of all browsers used worldwide in August. The only exception was IE10, the browser bundled with the new Windows 8, which does not contain the bug. Microsoft acknowledged it was investigating reports of a vulnerability but it did not promise a patch. The bug, when Microsoft patches it, will be rated "critical." Exploiting the flaw allows hackers to execute code and opens Windows XP, Vista, and Windows 7 to drive-by attacks that only require getting victims to visit a malicious or compromised Web site. Until a patch is available, Microsoft recommends users block attacks with EMET 3.0 (Exploit Mitigation Experience Toolkit), boost IE's security zone settings to "high," and configure the browser to display a warning before executing scripts.

Source: http://www.computerworld.com/s/article/9231396/Microsoft_confirms_hackers_exploiting_critical_IE_bug_promises_patch

40. *September 18, The H* – (International) **Apple fixes VNC security problem in Remote Desktop 3.5.** September 17, Apple released an update to the 3.5.x branch of its Apple Remote Desktop (ARD) administration application to close a known security hole. Version 3.5.3 of the desktop management solution for remotely managing Mac OS X systems corrects an information disclosure vulnerability (CVE-2012-0681) when connecting to third-party VNC servers that could result in data not being encrypted when the "Encrypt all network data" setting is enabled. When this happens, no warning is presented to alert users that the connection could be insecure.
Source: http://www.h-online.com/security/news/item/Apple-fixes-VNC-security-problem-in-Remote-Desktop-3-5-1710538.html

41. *September 17, Infoworld* – (International) **Jenkins integration server suffers security vulnerabilities.** Jenkins, the open source continuous integration server, faced several security vulnerabilities September 17, with the Jenkins project leader recommending upgrades to the Jenkins core and some plug-ins to fix the problems. A security advisory posted by the project leader cites four vulnerabilities, including two affecting the Jenkins core. The first vulnerability was deemed critical. It "allows unprivileged users to insert data into Jenkins master, which can lead to remote code execution. For this vulnerability to be exploited, the attacker must have an HTTP access to a Jenkins master, and he must have a read access to Jenkins," the security advisory said. The second vulnerability in the core involves a cross-site scripting vulnerability, allowing an attacker to craft a URL that points to Jenkins, with an attacker able to hijack a legitimate user's session. Two other vulnerabilities, also involving cross-site scripting, affect the Violations and Continuous Integration Game plugins. The Violations plug-in scans for violation XML files in the build workspace; the Game plug-in offers tips on improving builds.
Source: http://www.computerworld.com/s/article/9231372/Jenkins_integration_server_suffers_security_vulnerabilities

42. *September 17, eSecurity Planet* – (International) **Mobile emphasis at HP's Pwn2Own.** September 19, HP planned to host its first mobile Pwn2Own hacking competition at the EUSecWest event in Amsterdam, Netherlands. The event will challenge security professionals to find and exploit flaws in mobile technology for cash and prize awards. The contest will take aim at mobile Web browsers, near field communication (NFC), and Short Message Service (SMS), as well as cellular baseband technologies. Apple iOS, Blackberry, and Android smartphones will be among the devices under attack. HP will award the largest prize in the mobile Pwn2own contest to the researcher who can demonstrate a cellular baseband vulnerability.
Source: http://www.esecurityplanet.com/hackers/mobile-emphasis-at-hps-pwn2own.html

43. *September 17, Threatpost* – (International) **New iteration of TDSS/TDL-4 botnet uses domain fluxing to avoid detection.** A new version of the TDSS/TDL-4 botnet is rapidly growing, primarily because it is having success using an evasion technique known as a domain generation algorithm (DGA) to avoid detection, researchers at Damballa Security revealed September 17. The algorithm helps the latest version of the botnet conduct click-fraud campaigns and is used primarily to rapidly move communication between victims and command-and-control servers from domain to domain, a technique known as domain fluxing, similar to fast fluxing. Since this new version appeared in May, it has reportedly infected 250,000 unique victims, including machines inside government agencies, ISP networks, and 46 of the Fortune 500. Damballa researchers said they found 85 command and control servers and 418 domains related to the new version, primarily hosted in Russia, Romania, and the Netherlands.
Source: http://threatpost.com/en_us/blogs/new-iteration-tdsstdl-4-botnet-uses-domain-fluxing-avoid-detection-091712

For more stories, see items **7**, **8**, **10**, and **44**

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

44. *September 17, Threatpost* – (National) **Developer warns millions of Virgin Mobile subscribers about authentication flaw.** An Alamo, Texas developer September 17 warned Virgin Mobile U.S. subscribers that their accounts can be hacked after the company failed to respond with a fix. “I reported the issue to Virgin Mobile a month ago and they have not taken any action, nor informed me of any concrete steps to fix the problem, so I am disclosing this issue publicly,” he said in a blog post. He said he found that the carrier’s current authentication method relied on the user’s phone number and a six-number PIN to access an account. Using his own account, he created a script to narrow in on the 1 million possible passwords. Once the script unlocked his numeric PIN he realized “pretty much anyone can log into your Virgin Mobile account and wreak havoc, as long as they know your phone number.” He said he contacted the firm and its parent, Sprint, in August to alert them to the issue but became frustrated with the pace of the investigation and lack of communication. After several emails back and forth with a Sprint official, he was told September 14 the company did not plan further action on Virgin Mobile’s end.
Source: http://threatpost.com/en_us/blogs/developer-warns-millions-virgin-mobile-subscribers-about-authentication-flaw-091712

For more stories, see items **8** and **42**

[Return to top]

Commercial Facilities Sector

45. *September 18, WTXF 29 Philadelphia* – (Pennsylvania) **Coatesville fire kills mother and son, leaves dozens homeless.** Officials said a mother and son are dead and more than two dozen people were homeless after an overnight fire in Coatesville, Pennsylvania, WTXF 29 Philadelphia reported September 18. Several people were taken to nearby hospitals. A total of 31 people were displaced because of the fire. The Red Cross was at the scene helping them at a nearby shelter.
Source: http://www.myfoxphilly.com/story/19569999/fatal-3-alarm-fire-in-coatesville

46. *September 17, Orange County Register* – (California) **Fire burns warehouse in Santa Ana.** Fire crews contained a fire at a commercial warehouse in Santa Ana, California, September 17 that workers said was sparked while they were cutting metal. Firefighters responded to reports of a fire at Franco's Safe and Vault in an office park. The first units arrived to find heavy smoke and fire, and asked for additional crews to be sent, an Orange county fire authority official said. An explosion was reported, and a portion of the roof collapsed, officials said and forced crews to battle the fire from outside the building. Authorities closed Grand Avenue in both directions as they battled the flames. Firefighters stayed at the scene for several hours, mopping up after the fire. Workers at the safe and vault business said they were using cutting tools on metal when a spark struck an acrylic door, which was rapidly engulfed by the fire. The fire caused an estimated $500,000 in damage to the structure of the building, as well as $350,000 in damage to the building's contents. The fire damage was contained to the safe and vault business, although an adjacent pest-control business suffered water damage.
Source: http://www.ocregister.com/news/warehouse-371772-burns-fire.html

47. *September 14, Reuters* – (International) **Foreign journalists in China targeted by malware attacks.** Foreign journalists in Beijing, China, have been targeted by two very similar malware attacks in just over 2 weeks in the lead-up to China's once-in-a-decade leadership transition. The emails, one appearing to come from a Beijing-based foreign correspondent and the other from a Washington-based think tank, both contained an attachment with the same type of malware, according to an independent cyber security expert who reviewed the files. A government spokesman warned against jumping to conclusions about who was responsible. Both of the emails referred to the upcoming handover of power in the top ranks of the ruling Communist Party. The attachment, if opened, would have installed malware that sent encrypted information from the user's computer to an external server. That server is hosted in England.
Source: http://www.reuters.com/article/2012/09/14/us-china-malware-idUSBRE88D0CU20120914

For more stories, see items **10**, **43**, **48**, and **49**

[Return to top]

National Monuments and Icons Sector

48. *September 17, Associated Press; Yakima Herald-Republic* – (Washington) **Crews labor away on Yakima Complex blazes.** Work to prevent a fire burning west of Yakima, Washington, from growing went well September 17 as crews continued to establish fire breaks. But fire officials were unsure when it will be fully contained. Firefighters dug fire lines on the west end of the Wild Rose Fire, which is part of the Yakima Complex Fire burning east of Rimrock Lake. That fire was last reported at about 1,300 acres, but growth was minimal, said a Yakima Complex Fire spokesman. Meanwhile, another State team of roughly 350 firefighters that took over the Table Mountain Fire burning on about 2,500 acres near Blewett Pass in Kittitas County worked toward containment. Evacuations in the area remained in place September 17. That fire forced the closure of all land east of U.S. Highway 97 and south of U.S. Highway 2 in the Okanogan Wenatchee National Forest, according to a news release from fire officials overseeing the Yakima Complex Fire. Two firefighters suffered minor injuries. Both were treated at area hospitals and released, the news release said. Meanwhile in the Wenatchee area, an inversion moved in September 16, holding smoke in the region where 1,700 people were fighting a complex of wildfires burning on about 51 square miles. Hundreds of people have been evacuated. The Wenatchee complex was about 17 percent contained as of September 17. No homes had burned, but nearly 800 houses and other structures were threatened. The firefighting effort had so far cost an estimated $8.1 million.
Source: http://www.yakima-herald.com/stories/2012/09/17/crews-labor-away-on-yakima-complex-blazes

49. *September 17, Billings Gazette* – (Montana) **Crews continue mopping up on Dugan fire near Ekalaka.** Work reinforcing lines and mopping up on the 10,675-acre Dugan fire continued September 17. The fire, burning about 2 miles south of Ekalaka in and around Montana's Custer National Forest, has destroyed an uninhabited home, eight outbuildings, an uninhabited trailer, and three sheds since it started September 14. The fire's cause remains unknown and is under investigation. The fire also burned through the Ekalaka Park Campground. A U.S. Forest Service closure of National Forest System lands in the area impacted by the fire remained in effect.
Source: http://billingsgazette.com/news/state-and-regional/montana/crews-continue-mopping-up-on-dugan-fire-near-ekalaka/article_e714f502-a032-54ec-b844-c6ebf9d7f6de.html

50. *September 17, Casper Star-Tribune* – (Wyoming) **Local officials take lead on Casper Mountain fire, focus shifts to recovery.** With evacuations almost entirely lifted and all pre-evacuation notices cancelled, a fire management crew of mostly Wyoming land officials was managing what was left of the Sheep Herder Hill Fire, the Casper Star-Tribune reported September 17. Even with 100 percent containment, the Sheep Herder Hill Fire was not entirely out. For fire officials, this meant focus has moved from fire suppression to securing roads and still-standing structures from hazardous trees, and cooling hot spots around structures and fire lines.

Source: http://trib.com/news/local/casper/local-officials-take-lead-on-casper-mountain-fire-focus-shifts/article_44afc158-2bdd-5356-a371-4739b12290ef.html

[Return to top]

Dams Sector

51. *September 18, MLive.com* – (Michigan) **Plug the dikes to protect the lake: Muskegon County Drain Commissioner explains plan for Mona Lake.** The drain commissioner of Muskegon County, Michigan, said he is getting permits to plug holes in the dikes of the 200-acre celery flats on either side of Black Creek on the east end of Mona Lake, MLive.com reported September 18. A recent study found that about 70 percent of the phosphorus in Mona Lake came from the flats. Phosphorus promotes the growth of algae that is toxic to animals and aesthetically displeasing to humans. Phosphorus left over from when the area was a farm is still leaching into Mona Lake. The commissioner plans to plug the current holes in the dikes, but set them low enough so water will spill into Mona Lake during floods instead of ending up in people's yards and basements. Currently, the flats are connected to the lake and rise and fall with it, because the water that spills over during a flood will not contain much phosphorus.
    Source:
    http://www.mlive.com/news/muskegon/index.ssf/2012/09/plug_the_dikes_to_protect_the.html

[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.