



Homeland
Security

Daily Open Source Infrastructure Report

19 March 2012

Top Stories

- Utility officials said the “catastrophic failure” of an underground electrical cable led to a transformer explosion and fire March 13 that closed businesses, roads, and transit stations in downtown Boston. – *Beacon Hill Patch* (See item [1](#))
- Researchers have come across a new Android threat designed specifically to steal online banking credentials and create persistent, silent access to the compromised handset. – *ZDNet* (See item [13](#))
- Florence-Carlton school administrators shut down all 3 schools in Florence, Montana, for a few days after an outbreak of acute gastroenteritis sickened more than 100 students. – *Associated Press* (See item [37](#))
- The Sarasota, Florida police headquarters and several neighboring businesses were evacuated March 15 after police said a man showed up with a live hand grenade. – *WWSB 40 Sarasota* (See item [40](#))
- A confirmed working exploit for the MS12-020 RDP vulnerability in Windows is circulating. Experts say it is capable of either crashing or causing a denial-of-service condition on vulnerable machines. – *Threatpost* (See item [44](#))
- Security companies found multiple malware threats that use stolen digital certificates to sign components to avoid detection. – *IDG News Service* (See item [46](#))

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

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - <http://www.esisac.com>]

1. *March 16, Beacon Hill Patch* – (Massachusetts) **Fire cause: ‘castatrophic failure’ of cable.** The “catastrophic failure” of an underground electrical cable connected to a transformer at NStar’s Scotia Street substation in Boston, sparked the four-alarm fire March 13, NStar officials said March 15. Soot buildup in the backout transformer then caused the major blackout that cut off power to 21,000 customers across the Back Bay and surrounding downtown areas. The power was restored March 15. During the outage, NStar partnered with other utility companies to station about 60 generators across the neighborhood as a temporary fix to power homes, hotels, and businesses. Workers had to dig up the street to access the underground cables, and they also re-routed cables from another power station to jump-start the Scotia Street transformers, which were not damaged.
Source: <http://beaconhill.patch.com/articles/fire-cause-castatrophic-failure-of-cable-e2bdda90>
2. *March 15, WBKO 13 Bowling Green* – (Kentucky) **Oil well operators in Hart County indicted.** A federal grand jury in Bowling Green, Kentucky, returned a six-count indictment the week of March 12, against two oil drillers. They are charged with conspiracy to violate the Safe Drinking Water Act (SDWA) and violations of the SDWA. The indictment alleges that from March 13, 2008 to June 29, 2010, the men conspired with each other and others, to violate the SDWA by configuring piping to inject produced brine water (fluids brought to the surface in connection with oil production) from the tank battery to sinkholes and injecting produced brine water into sinkholes. The Indictment said the two men, and the corporation Logsdon Valley Oil Company, Inc., improperly conveyed and injected produced water into sinkholes in Hart County on March 13, 2008, December 10, 2009, May 24, 2010, and June 29,

2010. The two are charged with violation of the SDWA on oil production leases in Hart County.

Source:

http://www.wbko.com/news/headlines/Oil_Well_Operators_in_Hart_County_Indicted_142875265.html

3. *March 15, KTVZ 21 Bend* – (Oregon) **Hwy. 58 fuel tanker spill cleanup continues.** Highway 58 west of Oakridge, Oregon, will remain restricted to a single lane of travel into March 19 as authorities continue to clean up about 5,600 gallons of gas and diesel spilled from an overturned fuel tanker that ruptured, Oregon Department of Transportation (ODOT) officials said March 15. The ODOT said the latest estimate is 3,100 gallons of gasoline and 2,500 gallons of diesel spilled into a ditch along the south side of the highway. Personnel and equipment conducting the cleanup are accessing the area via the eastbound lane, necessitating the lane closure for safety. At this time, the ODOT said, it is uncertain how long the cleanup and lane closure will continue.
Source: <http://www.ktvz.com/news/30686956/detail.html>
4. *March 15, Salt Lake Tribune* – (Utah) **Semis crash, closing Highway 6 in Spanish Fork Canyon.** Spanish Fork Canyon in Utah was closed to traffic because of a collision between two semitrailer trucks, the Salt Lake Tribune reported March 15. One truck was hauling a load of gasoline, said a Utah Highway Patrol corporal. One person suffered minor injuries, and gasoline was leaking from one of the trucks. U.S. Highway 89 was also closed for about 40 miles south of the Highway 6 turnoff, where the incident occurred. The canyon was expected to remain closed for several hours.
Source: <http://www.sltrib.com/sltrib/news/53728729-78/highway-canyon-closed-fork.html.csp>

For more stories, see items [6](#), [26](#), and [38](#)

[\[Return to top\]](#)

Chemical Industry Sector

5. *March 16, WISH 8 Indianapolis* – (Indiana) **Fiery crash closes I-70 EB near Post Road.** An early March 16 crash caused a chemical spill and fire, and caused all lanes of I-70 near Post Road in Indianapolis to be closed for several hours. Eastbound lanes remained closed through the March 16 morning rush hour and were not expected to reopen until the early afternoon. The crash occurred when a semitrailer carrying 3,500 pounds of composite resin, known as UN #1866, crashed into a highway overhang sign, causing the truck to burst into flames. The driver told police a tire blowout led to the crash. He suffered serious burn injuries and was rescued by an ambulance crew that had been in a vehicle close beyond the truck when the crash happened. The driver was airlifted to a hospital and was listed in serious condition. The sign the truck hit was not structurally sound, so the transportation department planned to bring in a crane to remove it. HAZMAT crews said the resin was highly flammable and presented a respiratory threat. But most of the product was destroyed or burned on impact, so no

evacuations were ordered. HAZMAT crews reported most of the runoff from the resin spill had been contained. But some chemicals and diesel fuel were still present in a drainage ditch. State health and environmental officials cleaned the spill up.

Source: http://www.wishtv.com/dpp/news/local/marion_county/crash-at-i-70-traffic-rerouted

6. *March 16, Pekin Daily Times* – (Illinois) **Fire damages chemical facility.** Pekin, Illinois firefighters were called March 15 to put out a chemical fire at the Aventine Renewable Energy storage shed on Distillery Road. Responding firefighters found flames coming from the building and quickly extinguished them. The cause of the fire remains under investigation, said the Pekin fire chief. He said the fire did between \$20,000 to \$25,000 in damage to the building and a pump that transported chemicals to the main plant. None of the chemicals in the warehouse leaked or burned.
Source: <http://www.pekintimes.com/news/x1907515078/Fire-damages-chemical-facility>
7. *March 16, Athens News Courier* – (Alabama) **Truck driver ‘critical’ after wreck.** A man remained in critical condition late March 15 following a head-on collision with a fertilizer truck on Browns Ferry Road 1 mile south of Athens, Alabama. The morning accident caused a truck to overturn, spilling dry fertilizer onto the roadway, over a bridge, and onto mudflats below. The driver of the truck hauling fertilizer for Limestone Farmers Co-op in Athens suffered a minor injury. Fire crews and a HAZMAT team responded, but the co-op general manager said the fertilizer used for corn contained no explosive products. A co-op employee and others used grain shovels to remove the fertilizer from the road while emergency crews made sure there was no spark from the truck’s spilled diesel fuel and the fertilizer. The wreck halted traffic on Browns Ferry Road. A fire official said the Alabama Department of Environmental Management was notified of the spill and would be in charge of the clean up.
Source: <http://enewscourier.com/x426441953/UPDATE-Truck-driver-critical-after-wreck>
8. *March 16, Newark Advocate* – (Ohio) **Spill leaves one lane closed on Interstate 70.** One lane of Interstate 70 eastbound at Ohio 256 near Newark, Ohio, was expected to be closed until early March 16 while authorities dealt with a chemical fuel leaking from a tractor-trailer. The driver of the trailer hauling containers full of lye, also known as sodium hydroxide, was eastbound on I-70 early the evening of March 15 when the incident occurred. He said he felt his load had shifted and pulled over, according to an Ohio Highway Patrol news release. It said when he opened his trailer, he observed chemical fuel leaking. A HAZMAT team was called in and the eastbound lanes were closed. One lane was open shortly before midnight. About six emergency response agencies were on the scene.
Source: <http://www.newarkadvocate.com/article/20120316/NEWS01/203160310>

For another story, see item [26](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials and Waste Sector

9. *March 15, Washington Post* – (National) **Key nuclear plant safety order likely to be delayed, NRC tells Senate.** The Nuclear Regulatory Commission (NRC) will likely fall behind schedule in issuing a key safety measure designed for U.S. nuclear power plants, the agency’s chairman told a Senate committee March 15. The NRC’s five commissioners testified before the Senate’s Environment and Public Works Committee on the safety progress of the U.S. nuclear industry a year after an earthquake caused a nuclear disaster at Japan’s Fukushima Daiichi plant. The NRC chairman said U.S. nuclear power plants would likely miss the agency’s 5-year goal for implementing orders aimed at avoiding the effects of earthquakes on the plants. An agency task force on the Japanese disaster said the measures should be put in place at the nation’s 104 nuclear power plants by 2016. But the chairman said the earliest completion date for key seismic upgrades at the plants would be in 2017, and 2019 for low-risk plants.
Source: http://www.washingtonpost.com/blogs/federal-eye/post/key-nuclear-plant-safety-order-likely-to-be-delayed-nrc-tells-senate/2012/03/15/gIQAX5maES_blog.html

10. *March 15, Homeland Security Today* – (International) **Study cites lack of public-private coordination in Japanese nuclear accident response.** The response to the March 2011 earthquake and tsunami that crippled the Fukushima Daiichi Nuclear Power Station in Japan was exacerbated by communication gaps between the government and the nuclear industry, according to a new report in the Bulletin of the Atomic Scientists, Homeland Security Today reported March 15. The report found the government, Tokyo Electric Power Co. (TEPCO), and other relevant actors “were thoroughly unprepared on almost every level for the cascading nuclear disaster,” in part due to “dysfunction within and between government agencies and TEPCO, particularly in regard to political leadership and crisis management.” The investigation also found ambiguity about the roles of public and private institutions in the crisis was a factor in the poor response at Fukushima. The crisis also “revealed the dangers of building multiple nuclear reactor units close to one another.” This proximity, it explained, triggered the parallel, cascading accidents that led to hydrogen explosions blowing the roofs off of reactor buildings and water evaporating from the exposed spent fuel pools, “a situation that was potentially more dangerous than the loss of reactor cooling itself.” That failure may have stemmed from TEPCO’s most recent abnormal operating procedures, which were created in 1994 and did not address the possibility of a prolonged, total loss of power at a nuclear plant.
Source: <http://www.hstoday.us/briefings/today-s-news-analysis/single-article/study-cites-lack-of-public-private-coordination-in-japanese-nuclear-accident-response/d329d6360d8b7e0310ca9ecfaa533fbc.html>

[\[Return to top\]](#)

Critical Manufacturing Sector

See item [17](#)

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Banking and Finance Sector

11. *March 15, U.S. Securities and Exchange Commission* – (California) **SEC charges senior executives at California-based firm in stock lending scheme.** The Securities and Exchange Commission (SEC) charged two senior executives and their California-based firm March 15 with defrauding officers and directors at publicly-traded companies in an elaborate \$8 million stock lending scheme. The SEC alleges that Argyll Investments LLC’s purported stock-collateralized loan business is merely a fraud perpetrated by the executives to acquire publicly traded stock from corporate officers and directors at a discounted price from market value, separately sell the shares for full market value to fund the loan, and use the remaining proceeds from the sale of the collateral for their own benefit. The executives and Argyll lied to borrowers by explicitly telling them their collateral would not be sold unless a default occurred. However, since Argyll had no independent source of funds other than the borrowers’ collateral, it often sold the collateral prior to closing the loan and then used the proceeds to fund it. Also charged in the complaint is AmeriFund Capital Finance LLC and its owner who the SEC alleges violated securities laws by brokering many transactions for Argyll while not registered with the SEC. The SEC alleged the executives induced at least nine corporate officers and directors since 2009 to transfer ownership of millions of shares of stock to Argyll as collateral for purported loans. As a result of the scheme, Argyll reaped more than \$8 million in unlawful gains. Source: <http://www.sec.gov/news/press/2012/2012-46.htm>
12. *March 15, Associated Press* – (Ohio; National) **Ohio man pleads guilty in \$17M Amish fraud case.** An Ohio man admitted March 15 he defrauded fellow Amish in 29 states out of nearly \$17 million. A one-count mail fraud indictment returned in 2011 charged the man with promising investors safe securities but moving money to riskier investments. The indictment said nearly 2,700 people and entities, including an Amish community loan fund, lost about \$16.8 million since 2006. His company has filed for bankruptcy protection. The charge carries a maximum 20-year sentence. “[He] told the investors that their money would be used to purchase risk-free U.S. government securities, which would generate returns for the investors,” the Securities and Exchange Commission said in a 2011 civil filing. “In reality, [he] used the money to make speculative investments in high yield (junk) bonds, mutual funds, and stocks.” Source: <http://abcnews.go.com/US/wireStory/ohio-man-ready-change-plea-amish-fraud-case-15927230#.T2JOHnkehI4>
13. *March 15, ZDNet* – (International) **Remote-controlled Android malware stealing banking credentials.** Security researchers at McAfee have discovered a malicious Android application capable of grabbing banking passwords from a mobile device without infecting the user’s computer. The latest piece of Android Malware, dubbed

FakeToken, contains man-in-the-middle functionality to hijack two-factor authentication tokens and can be remotely controlled to grab the initial banking password directly from the infected mobile device. The malicious application targets specific well-known financial entities posing as a Token Generator application. When the application executes, it shows a Web view component that displays an HTML/JavaScript Web page that pretends to be a Token Generator. The page also appears to be from the targeted bank. To get the fake token, a researcher discovered the user must enter the first factor of authentication. “When the user clicks ‘Generate,’ the malware shows the fake token (which is in fact a random number) and sends the password to a specific cell phone number along with the device identifiers (IMEI and IMSI). The same information is also sent to one of the control servers along with further data such as the phone number of the device. The malware finds the list of control servers from an XML file inside the original APK,” he added. He said the malware also contains commands to update itself or spy on the infected machine. The researcher found the FakeToken app can also hijack the list of contacts stored in the device (name and number).

Source: <http://www.zdnet.com/blog/security/remote-controlled-android-malware-stealing-banking-credentials/10804>

14. *March 15, Associated Press* – (International) **Iran cut off from global financial system.** Dozens of Iranian banks were blocked from doing business with much of the world as the West tightens the financial screws on the country. The Belgium-based company that facilitates most international bank transfers took the unprecedented step March 15 of blocking 30 Iranian banks from using its service. The move is likely to hurt Iran’s all-important oil industry and make it difficult for citizens to receive money from relatives living abroad. The move by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is part of a broader effort by Western nations to isolate Iran financially and force it to demonstrate it is not trying to develop nuclear weapons. The SWIFT said it was forced by recent European Union sanctions to discontinue service to Iranian banks beginning March 17. The SWIFT is a secure private network used by nearly every bank around the world to send payment messages that lead to the transfer of money across international borders.

Source: <http://www.kansascity.com/2012/03/15/3492507/swift-financial-service-cuts-ties.html>

15. *March 15, KGAN 2 Cedar Rapids; KFXA 28 Cedar Rapids* – (Iowa) **TV producer convicted of fraud in Iowa film tax credit scandal.** A Nebraska film and video producer has been convicted in Iowa of taking more than \$9 million in state tax credits for a TV series on training horses, KGAN 2 and KFXA 28 Cedar Rapids reported March 15. The defendant was convicted of fraudulent practice in the first degree, and was acquitted of two other charges. The state alleged the defendant took more than \$9.1 million in film tax credit certificates, and produced just five television shows and DVD’s on horse training. He credited himself as the primary producer and lead on-screen talent for the documents. In January, he was charged with knowingly making false statements to get the tax credits. He faces up to 10 years in prison and a \$10,000 fine.

Source:

http://www.kgan.com/shared/newsroom/top_stories/videos/kgan_vid_10356.shtml

16. *March 14, Fort Lauderdale Sun-Sentinel* – (Florida) **Fugitive Brinks impostor sought for Black Friday robbery.** A reward is being offered for information leading to the arrest of a man who posed as an armed Brinks security guard to steal cash from a clothing store at the Sawgrass Mills mall in Sunrise, Florida, November 26, 2011, according to Sunrise police. The suspect walked into the Aeropostale store and walked out with \$162,000, investigators said. Sunrise police believe he had inside knowledge of the operation and knew there would be a lot of cash on hand after the busiest shopping day of the year. The robbery went undetected until police found a stolen getaway car with a gun, belt, cap, and the very convincing homemade Brinks uniform the robber used to fool the store manager, detectives said.

Source: http://articles.sun-sentinel.com/2012-03-14/news/fl-fugitive-brinks-impostor-folo-20120314_1_impostor-brinks-security-guard-getaway-car

[\[Return to top\]](#)

Transportation Sector

17. *March 15, Fly Away Simulation* – (National) **FAA proposes wiring change on Boeing 737.** The U.S. Federal Aviation Administration (FAA) proposed changes on the overhead panel and wiring for Next Generation Boeing 737 aircraft, Fly Away Simulation reported March 15. This follows reports that three pilots failed to manually activate air data sensor heating systems on the aircraft as part of a pre-takeoff checklist procedure. “The affected airplanes do not have an automatic activation of the air data sensor heating system,” said the FAA. “Pilots activate the system manually as a pre-takeoff checklist item. Failure to activate the air data sensor hearing system could result in ice formation on air data system sensors, which could lead to misleading airspeed data or loss of all airspeed indicating systems, and loss of control of the airplane.” According to FAA estimates, these changes would take 80 hours per aircraft to implement, and will cost about \$15 million for the 1,025 Boeing aircraft in the U.S.-registered fleet. These changes would need to be implemented within 2 years.

Source: <http://flyawaysimulation.com/news/4392/faa-proposes-wiring-change-on-boeing-737/>

18. *March 15, Cannon Beach Gazette* – (Oregon) **City Council: No replacement for the Ecola Creek Bridge.** The city council in Cannon Beach, Oregon, decided not to replace the Ecola Creek Bridge with an earthquake resistant bridge; rather, the city plans to wait until the current bridge is due for replacement 10 to 15 years from now, the Cannon Beach Gazette reported March 15. The concrete deck bridge stands on wood pilings and was built in 1964 following the Alaskan earthquake that spawned a tsunami that destroyed the old bridge. The Ecola Creek Bridge was determined to be unstable in the event of an earthquake, and is not expected to withstand strong shaking. The bridge is adjacent to the Cannon Beach Elementary School and the Christian Conference Center. It would be the quickest evacuation route to higher ground for students and staff of the school, as well as residents, businesses, and visitors in the

north end of downtown.

Source: http://www.cannonbeachgazette.com/news/local_news/article_320ed48a-6eff-11e1-a872-0019bb2963f4.html

For more stories, see items [1](#), [3](#), [4](#), [5](#), [7](#), [8](#), and [58](#)

[\[Return to top\]](#)

Postal and Shipping Sector

19. *March 15, Associated Press* – (Georgia) **Mail worker runs for cover after pellet shot.** Police in Lawrenceville, Georgia, said a teenager is accused of shooting a pellet gun at a mail truck, leading the postal worker inside to run for cover after his windshield was cracked by one of the shots. The Gwinnett Daily Post reported the shooting happened March 12. The teen is charged with aggravated assault with an offensive object, terroristic threats and acts, and interference with government property. Police said the postal worker was collecting and delivering mail to mailboxes when he heard a “ping” sound, then saw his windshield crack at eye-level. Police said he then ran down the street and hid while calling police. Authorities said a responding officer spotted an open window above a garage at a nearby house, leading to the suspect’s apprehension.

Source: http://www.actionnewsjax.com/content/topstories/story/Mail-worker-runs-for-cover-after-pellet-shot/LAo8iMZ2_EiQS-nfuHCG2g.csp

[\[Return to top\]](#)

Agriculture and Food Sector

20. *March 16, Associated Press* – (Nebraska) **Co-op pleads guilty in Stanton worker’s death.** A co-op must pay penalties totaling nearly \$187,000 over the death of a worker at a northeast Nebraska grain elevator. Federal prosecutors said Farmers Union Cooperative Supply was sentenced March 16. The co-op had pleaded guilty to willfully violating federal safety regulations, causing the death of an employee. A man was found dead inside a grain pit at the co-op elevator in Stanton June 19, 2009. An autopsy showed he asphyxiated. Authorities said the co-op knew the safety rules regarding oxygen levels in confined areas but did not follow them. The co-op was fined \$100,000 for the criminal violation and placed on probation. The company also has agreed to pay a civil penalty of nearly \$87,000.

Source: <http://www.ketv.com/r/30692799/detail.html>

21. *March 15, Food Safety News* – (International) **Allergen alert: Sulfites in dried fungus.** The Canadian Food Inspection Agency and importer Canadian T & J International Development of Richmond, British Columbia, are warning people with sensitivity to sulphites not to eat certain Natural World brand Dried Fungus because it contains sulphites that are not listed on the labels, Food Safety News reported March 15.

Source: <http://www.foodsafetynews.com/2012/03/allergen-alert-sulfites-in-dried-fungus/>

22. *March 15, Food Safety News* – (International) **Allergen alert: Cheetos with milk, soy.** The Canadian Food Inspection Agency and PK Trading of Mississauga, Ontario, are warning people with allergies to milk or soy not to consume certain Frito Lay Cheetos because they contain milk and soy, which are not declared on the label, Food Safety News reported March 15. All codes of the following Frito Lay brand Cheetos products, imported from Korea, are affected by this alert: Cheetos (BBQ flavor, red bag) and Cheetos (Hot flavor, black bag). The recalled Cheetos were distributed in Ontario and Manitoba.
Source: <http://www.foodsafetynews.com/2012/03/allergen-alert-cheetos-with-milk-soy/>
23. *March 15, Food Safety News* – (International) **Canada E. coli beef recall expands again.** Canadian health authorities are once again expanding a recall of certain beef products as part of an ongoing E. coli O157:H7 investigation, Food Safety News reported March 15. One illness was reported in connection with these products. The Canadian Food Inspection Agency and New Food Classics are warning the public not to consume certain Best Value beef burgers because they may be contaminated with E. coli O157:H7. The recalled burgers were distributed to Giant Tiger and Northern Canada retail stores in British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, Newfoundland, Labrador, Northwest Territories, and Nunavut.
Source: <http://www.foodsafetynews.com/2012/03/canada-e-coli-beef-recall-expands-again/>
24. *March 15, Food Safety News* – (New Jersey) **Pregnant woman's Listeria case prompts cheese recall in NJ.** A woman 38 weeks pregnant was diagnosed with Listeria monocytogenes infection, and the New Jersey Department of Health and Senior Services (NJDHSS) is now warning the public not to eat any cheese products produced by El Ranchero del Sur of South River, New Jersey, Food Safety News reported March 15. Lab tests confirmed L. monocytogenes in a sample of the company's Los Corrales Queso Fresco Fresh Cheese and Banana Leaf, according to the NJDHSS. The pregnant woman's Listeria infection was diagnosed March 2. El Ranchero del Sur agreed to recall its products and close its production plant. While the facility is inspected, all products and ingredients have been embargoed, state public health officials said. According to the news alert, El Ranchero del Sur cheese products are found primarily in Mexican and Latin American grocery stores, restaurants, and other Hispanic food establishments under the name brands El Ranchero, Los Corrales, and Carnes Don Beto.
Source: <http://www.foodsafetynews.com/2012/03/listeria-case-prompts-cheese-recall-in-new-jersey/>

For more stories, see items [7](#) and [56](#)

[\[Return to top\]](#)

Water Sector

25. *March 16, WPBF 25 West Palm Beach* – (Florida) **More than 40,000 Seacoast Utility customers under boil-water alert.** Some Palm Beach Gardens, Florida businesses were forced to close because of a boil-water alert issued March 15. More than 40,000 Seacoast Utility Authority customers are affected. Seacoast Utility Authority said the boil-water alert is a precaution due to a water-main break from construction at the Hood Road water treatment plant March 15. The precautionary boil water notice will remain in effect until the problem has been corrected and a bacteriological survey shows the water is safe for use.
Source: <http://www.wpbfb.com/news/south-florida/Palm-Beach-County-News/More-than-40-000-Seacoast-Utility-customers-under-boil-water-alert/-/8815578/9331416/-/item/0/-/dx2smez/-/index.html>
26. *March 16, Associated Press* – (California) **Water board OKs \$6.3M PG&E toxic settlement claim.** A Southern California water board has agreed to accept \$3.6 million from Pacific Gas & Electric (PG&E) to settle claims the utility failed to stem toxic chromium pollution in a Mojave Desert city. The settlement was approved March 14 by the Lahontan Regional Water Quality Control Board. The board claimed the utility failed to contain a plume of chromium 6 that polluted the Hinkley water supply. PG&E once used chromium 6 to reduce corrosion at cooling towers. PG&E agreed to contain the pollution, but the water board says the plume has grown.
Source: <http://www.mynews4.com/news/story/Water-board-OKs-6-3M-PG-E-toxic-settlement-claim/ucjTzKC0jEi2pRPCPNjLwQ.csp>
27. *March 15, Associated Press* – (Pennsylvania) **EPA: Water quality OK in Pa. gas drilling town.** Federal environmental regulators said well water testing at 11 homes in a northeastern Pennsylvania village where a gas driller was accused of polluting the aquifer failed to show elevated levels of contamination. The Environmental Protection Agency is sampling well water at dozens of homes in Dimock, Susquehanna County. The agency said March 15 it received initial test results for 11 homes. Regulators said water samples from six of the 11 homes showed sodium, methane, chromium or bacteria, but at safe levels. Arsenic was found in the well water of two homes but at low levels.
Source: <http://online.wsj.com/article/AP977e9c6d3cb74a9cb030fe9bb7d32d15.html>
28. *March 15, Hanford Sentinel* – (California) **Suspects wanted in costly crash on city property.** Police are looking for three men who stole a pickup truck March 13 in Hanford, California, drove it a block away, and crashed into a sump pump station, causing thousands of dollars in damage. City officials estimate the damage to the facility at Tempe Drive and Anacapa Avenue to be around \$21,000. Witnesses reported seeing three men fleeing from the scene, but no suspect descriptions have been given.
Source: http://www.hanfordsentinel.com/news/local/suspects-wanted-in-costly-crash-on-city-property/article_e5eff766-6ed4-11e1-8dc5-001871e3ce6c.html

For more stories, see items [2](#), [35](#), and [58](#)

[\[Return to top\]](#)

Public Health and Healthcare Sector

29. *March 16, Columbus Dispatch* – (Ohio) **Man admits he beat two women at care facility.** A man admitted March 15 to breaking into a North Side assisted-living center in Columbus, Ohio, and beating two women. The man used a large wooden stake to break out a glass door at InCare Suites, August 7, and then went into the lobby and began beating two residents with the stake. One 64-year-old woman suffered a fractured skull and cheekbone, the second resident, 81, had broken bones in both of her forearms.
Source: <http://www.dispatch.com/content/stories/local/2012/03/16/man-admits-he-beat-two-women-at-care-facility.html>
30. *March 15, Augusta Chronicle* – (Georgia) **Stolen laptop had patient records from MCG Hospital clinic.** The records of 513 patients at Medical College of Georgia Hospital and Clinics in Augusta, Georgia, were on a laptop stolen during a January 18 burglary, the school announced March 15. The laptop was used by a nurse practitioner who travels to other clinics in Georgia and had permission to have patient records on the computer. The laptop was not encrypted, but “the risk is relatively low” for identity theft because the records did not contain financial data, addresses, or Social Security numbers, the chief integrity officer said. All of the 513 patients were in the adult sickle cell clinic and all have been notified.
Source: <http://chronicle.augusta.com/news/crime-courts/2012-03-15/stolen-laptop-had-patient-records-mcg-hospital-clinic?v=1331853486>
31. *March 14, Nature News* – (National; International) **Drug data reveal sneaky side effects.** An algorithm designed by U.S. scientists to trawl through a plethora of drug interactions has yielded thousands of previously unknown side effects caused by taking drugs in combination. The work, published March 14 in Science Translational Medicine, provides a way to sort through the hundreds of thousands of “adverse events” reported to the Food and Drug Administration (FDA) each year. The team compiled a database of 1,332 drugs and possible side effects not listed on the labels for those drugs. On average, the program found 329 side effects for every drug, when most drug labels list an average of 69 effects. The new program, developed at Stanford University, combs through millions of doctor and patient reports to the FDA, Canada’s MedEffect, and similar databases.
Source: <http://www.nature.com/news/drug-data-reveal-sneaky-side-effects-1.10220>

[\[Return to top\]](#)

Government Facilities Sector

32. *March 16, Tinley Park Southtown Star* – (Illinois) **Police: Matteson school locked down after parent’s death threat.** A Matteson, Illinois elementary school was locked down March 15 for about 4 hours after a man threatened to kill anyone who tried to stop him from picking up his 2 children at the school, police said. The lockdown

- occurred at Marya Yates School, the Matteson police chief said. Police said a restraining order bans the man from seeing his family, and he told a school clerk during a phone call that he was picking up his kids from the school and would “kill anybody in his way.” A school employee recognized the man’s voice and identified him to police. Police tracked his phone and arrested him in Chicago, and the lockdown was lifted. Source: <http://southtownstar.suntimes.com/neighborhoodstar/matteson/11317150-418/police-matteson-school-locked-down-after-parents-death-threat.html>
33. *March 16, Associated Press* – (Indiana) **Softball player improving after lightning strike.** A southern Indiana high school freshman was on the mend after being struck by lightning as she and other members of a girls softball team were practicing outside Seymour High School in Seymour, the Associated Press reported March 16. The Seymour Community Schools superintendent told the Tribune of Seymour that the freshman was taken to a hospital in Indianapolis after lightning struck her March 15. A hospital spokesman said March 16 the girl was admitted in critical condition, but she was upgraded to good condition. Three other girls were taken to a hospital after the lightning strike, complaining of headaches, but they were released March 15. The Seymour police chief said skies were clear at the time of the lightning strike about 50 miles south of Indianapolis. Source: <http://www.oregonlive.com/newsflash/index.ssf/story/softball-player-improving-after-lightning-strike/838023990c8340b597a031b42c803bd9>
34. *March 16, Port Townsend & Jefferson County Leader* – (National) **U.S. Navy hosting ‘mass casualty’ exercise with local agencies March 19.** Local emergency response entities are taking part in one segment of a major training exercise the week of March 19 at Naval Magazine Indian Island in Washington state. A nationwide U.S. Navy exercise called Solid Curtain-Citadel Shield 2012 is being conducted on the island and other naval bases throughout the continental United States from March 19 to March 24. The annual exercise is designed to enhance training and readiness of Navy security forces to respond to threats to installations and units, said a Navy press release. It will cause gate closures, delays in base access, and increased security activity at Navy facilities from March 22 to March 24, according to a March 5 Navy press release. Naval Magazine Indian Island has partnered with several organizations in Jefferson County to explore additional training opportunities by using Navy resources being made available for the exercise. Source: <http://www.ptleader.com/main.asp?SectionID=36&SubSectionID=55&ArticleID=31087>
35. *March 16, Knoxville News Sentinel* – (Tennessee) **City of Maryville fines Pellissippi State \$40,000 in coolant dumping.** Pellissippi State Community College officials are considering their options after the city of Maryville, Tennessee, fined the school \$40,000 for the illegal dumping of coolant chemicals into the city sewer system by Blount County campus personnel, the Knoxville News Sentinel reported March 16. The four prohibited discharges of HVAC system coolant occurred March 5 to 8, according to an environmental compliance inspector for the City of Maryville Water Quality Control. The inspector sent a notice of violation letter March 13. The city manager sent

- a civil penalty assessments letter March 15 explaining that officials have 30 days to appeal. Officials said personnel at the campus knowingly discarded the chemicals after a supervisor was warned against it. The city manager recommended the school be fined \$10,000 for each violation. Officials said the discharges totaled about 450 gallons.
Source: <http://www.knoxnews.com/news/2012/mar/16/city-of-maryville-fines-pellissippi-state-40000/>
36. *March 15, Parsippany Daily Record* – (New Jersey) **Sussex Tech in Sparta closed after fire in science classroom.** Sussex County Technical School in Sparta, New Jersey was closed March 15 after a March 14 fire that severely damaged a science classroom, police said. The township police communications center received a fire alarm activated by smoke detectors, said a news release from the police department. A janitor reported a heavy smoke condition. Fire crews found a second-floor biology, chemistry, environmental lab filled with thick smoke, and flames coming from the base of a work table. The fire was quickly extinguished and the classroom was ventilated though it sustained heavy fire, smoke, and water damage. An adjoining classroom also sustained heavy damage, police said. The cause of the fire was determined to be “nonsuspicious” after an investigation. The fire appears to have started in a plastic garbage can after a chemical reaction occurred inside the container.
Source: <http://www.dailyrecord.com/article/20120315/NJNEWS/303150016/Sussex-Tech-Sparta-closed-after-fire-science-classroom?odyssey=nav|head>
37. *March 15, Associated Press* – (Montana) **Florence-Carlton school district closed due to gastroenteritis outbreak.** Florence-Carlton school administrators shut down all three schools in Florence, Montana, for the rest of the week after about 110 students called in sick March 15. The superintendent said several students went home sick March 14, but more than 10 percent of the student body was sick March 15. Parents were called shortly before noon March 15 to pick up students. The Ravalli County public health director said the health department planned to conduct a communicable disease investigation after students became ill with acute gastroenteritis. The superintendent said health officials instructed him to shut down the elementary school, middle school, and high school, and all school-related activities for the rest of the week. Classes were scheduled to resume March 19.
Source:
<http://www.therepublic.com/view/story/4dbafe6e1bcf4dd8be18fec5f6fde631/MT--Schools-Close-Illness/>
38. *March 14, Ruidoso News* – (New Mexico) **Hondo schools evacuated.** A propane gas leak March 14 forced the evacuation of the Hondo Valley Public Schools campus in Tinnie, New Mexico. Students were transported to the Tinnie Baptist Church where parents picked up their children. Classes were cancelled for the remainder of the day. A crew from a propane company turned off the gas and was looking for a possible leak. The tank is on the southeast corner of the campus. Only the campus and its buildings were evacuated. In addition to the Lincoln County Office of Emergency Services, the Hondo Volunteer Fire Department, and the Lincoln County Sheriff’s Office responded to the gas leak. The district has more than 150 students.

Source: http://www.ruidosonews.com/ruidoso-breaking_news/ci_20171877/hondo-schools-evacuated

39. *March 13, University of Tampa* – (Florida) **Data breach.** The office of information technology (IT) at the University of Tampa (UT) learned March 13 that a data file containing sensitive information was publicly accessible for a certain period due to a server management error. There is no evidence the file was used maliciously. Immediately after receiving notification, IT secured the file and took steps to ensure it was no longer accessible or searchable. The file included 6,818 records of Fall 2011 students. Information included UT identification number, Social Security number, name, and date of birth. The sensitive data was displayed as a string of numbers that would not be immediately obvious to a casual viewer. Exposure of this file was potentially from July 2011 through March 13. The compromised data was discovered during an in-class exercise and was immediately reported to IT. UT notified Google to remove the cached file from the search engine.

Source: <http://www.ut.edu/databreach/>

[\[Return to top\]](#)

Emergency Services Sector

40. *March 16, WWSB 40 Sarasota* – (Florida) **Man brings live grenade to Sarasota police headquarters.** The Sarasota, Florida police headquarters was evacuated March 15 after police said a man showed up with a live hand grenade. The man found the grenade inside of a paper bag in his front yard. He transported it to the police department. Once he arrived at the police department, he placed the grenade on top of the hood of his vehicle. As he was approaching the front desk officer, he came into contact with a lieutenant. The man told the lieutenant he had a grenade on the hood of his vehicle, and the lieutenant verified it was in fact a grenade. All surrounding businesses as well as the police department were evacuated. The grenade was detonated in a secure location by the Sarasota Police Department's Explosive Materials Unit.
- Source: <http://www.mysuncoast.com/content/topstories/story/Man-brings-live-grenade-to-Sarasota-Police/mf9uX60OikC6igtHpXHCEQ.csp>

41. *March 14, Chillicothe Gazette* – (Ohio) **Two dead in ambulance crash.** Two people were killed in Chillicothe, Ohio, March 14 after the private ambulance they were traveling in smashed into the back of a flatbed truck carrying lumber. The two were killed when the Life Ambulance struck a stopped flatbed truck at an intersection. According to a sergeant of the Ohio Highway Patrol, one man was headed south in the flatbed truck when he slowed and stopped to turn left. The other man was also headed south, and the sergeant said he failed to stop in time, striking the back of the truck with a full-frontal impact. The lumber on the back of the truck went through the ambulance's windshield and halfway through the ambulance, causing two people to suffer fatal head injuries. Both were pronounced dead at the scene by the Ross County coroner.

Source:

<http://www.chillicothegazette.com/article/20120314/NEWS01/120314002/Two-dead-ambulance-crash?odyssey=mod|mostview>

For another story, see item [18](#)

[\[Return to top\]](#)

Information Technology Sector

42. *March 16, Help Net Security* – (International) **Fake Google Play site serves Android malware.** The recent name change of Google’s official Android Market — now called Google Play — has been recently taken advantage of by scammers, Help Net Security reported March 16. According to Trend Micro researchers, fake Russian versions of the redesigned site have already appeared. “Download Google Play for Android Google Play is formerly known as the android market but now a vast and influential old android market combined with a store of books google ebookstore multi-format films and world music google music,” it is explained on the site. Among the suspicious Android apps offered for download is a Google Play application (google-play.apk), which is actually a Trojan that subscribes the victim to premium number services without asking his or her permission. The researchers said even if the Trojan in question is very similar to one discovered in February that has polymorphic abilities, this one does not, but tries to avoid detection by having various innocuous files added to it.
Source: http://www.net-security.org/malware_news.php?id=2036
43. *March 16, Softpedia* – (International) **Microsoft addresses Flash component vulnerability in Bing.** Three Vulnerability Lab researchers worked together to find and demonstrate a critical editor Flash component vulnerability on Microsoft’s Bing Service Application. The security experts identified the critical severity flaw and reported it to Microsoft February 7. Microsoft responded 2 days later, and March 14 the issue was addressed. If unaddressed, the remotely exploitable Flash component vulnerability may have allowed an attacker to implement malicious persistent comments while the user was editing or posting via Flash. The vulnerable module was the Comments&Edit — Flash Input/Output when swf files created with Action Script were loaded.
Source: <http://news.softpedia.com/news/Microsoft-Addresses-Flash-Component-Vulnerability-in-Bing-258952.shtml>
44. *March 16, Threatpost* – (International) **MS12-020 RDP exploit found, researchers say code may have leaked from security vendor.** There is a confirmed legitimate working exploit for the MS12-020 RDP vulnerability in Windows circulating already and researchers say it is capable of either crashing or causing a denial-of-service (DoS) condition on vulnerable machines, Threatpost reported March 16. Microsoft warned customers about the possibility of the exploit surfacing quickly and advised them to patch the flaw immediately. The researcher who discovered the vulnerability said the packet he included in his original advisory was found in the exploit, raising the specter of a data leak somewhere in the pipeline. The exploit surfaced on a Chinese download

site in the last few days and researchers have been able to confirm it causes a blue screen of death (BSOD) on some systems, and a DoS condition on other versions of Windows. Experts said the RDP bug, which was discovered by an Italian researcher, has the potential to be used as the basis for a large-scale worm and the existence of a working exploit is the first step down that road. The exploit will produce a BSOD on Windows 7 and a DoS on Windows XP.

Source: http://threatpost.com/en_us/blogs/ms12-020-rdp-exploit-found-researchers-say-code-may-have-leaked-security-vendor-031612

45. *March 15, SecurityWeek* – (International) ‘**Anonymous OS’ taken offline due to security concerns.** SourceForge removed a controversial Ubuntu-based operating system from its Web site due to claims the software is laced with trojans. Dubbed “Anonymous-OS,” the operating system was downloaded from SourceForge nearly 40,000 times before it was taken down. Affiliates of the Anonymous collective, however, have been quick to criticize the package. One of the more popular Anonymous Twitter accounts, AnonOps, declared March 14 the so-called AnonOS was fake and “wrapped in Trojans.” Another account, YourAnonNews, warned users the group “can’t vouch for it.” The OS came with pre-installed tools that can be used for password cracking and scanning for database vulnerabilities. It also included tools such as Tor that can be used to disguise someone’s online activities. In a statement on their site, the SourceForge team said it normally does not pass judgment on a download based on what someone using it could possibly do, but decided to act after security experts verified it was a security risk “and not merely a distribution of security-related utilities, as the project page implies.”

Source: <http://www.securityweek.com/anonymous-os-taken-offline-due-security-concerns>

46. *March 15, IDG News Service* – (International) **Digitally signed malware is increasingly prevalent, researchers say.** Security companies recently identified multiple malware threats that use stolen digital certificates to sign their components in an attempt to avoid detection and bypass Windows defenses, IDG News Service reported March 15. When it was discovered in 2010, the Stuxnet industrial sabotage worm surprised the security industry with its use of rootkit components that were digitally signed with certificates stolen from semiconductor manufacturers Realtek and JMicron. Security experts predicted at the time that other malware creators would adopt the technique to bypass the driver signature enforcement in 64-bit versions of Windows Vista and 7. Given recent developments it appears they were right. A backdoor discovered by Symantec in December 2011 installed a rootkit driver signed with a digital certificate stolen from an undisclosed company. The certificate was revoked by VeriSign at the owner’s request 9 days later. However, the time window available for the malware to remain undetected was larger than that, because Windows operating systems rarely check certificate revocation lists, or do not check them at all, Symantec’s principal software engineer said March 15.

Source:

http://www.computerworld.com/s/article/9225237/Digitally_signed_malware_is_increasingly_prevalent_researchers_say?taxonomyId=17

47. *March 15, IDG News Service* – (International) **Tech support scammers target antivirus customers, diversify tactics.** Tech support scammers have started targeting antivirus customers and have diversified their techniques, according to reports from antivirus vendors Avast and ESET. According to a March 15 IDG News Service report, cold-calling scams that target English-speaking computer users have been a common occurrence during the past 2 years. The scammers usually pose as tech support engineers who work for Microsoft or Internet service providers in an attempt to trick victims into buying questionable security or PC optimization software. However, it appears these attacks are becoming increasingly more targeted, with callers beginning to impersonate employees from companies that users already entrusted with their computers' protection.

Source:

http://www.computerworld.com/s/article/9225230/Tech_support_scammers_target_antivirus_customers_diversify_tactics?taxonomyId=17

48. *March 15, H Security* – (International) **Cisco closes holes in its Security Appliances.** Network equipment manufacturer Cisco is warning of a critical vulnerability in its ASA 5500 Series Adaptive Security Appliances (ASA) that could be exploited by a remote, unauthenticated attacker to execute arbitrary code and compromise a victim's system, the H reported March 15. The problem is located in a Cisco port forwarding ActiveX control — distributed to client systems by ASA as part of the Clientless VPN feature — that can be used to cause a buffer overflow. For an attack to be successful, a victim must first visit a specially crafted Web page in Internet Explorer or another Web browser that supports ActiveX technologies. Versions 7.1 and 7.2, as well as 8.0 to 8.6 of the Cisco ASA software are affected. Cisco contacted Microsoft and requested it set a global kill bit for the vulnerable control in a future update, which will disable the exploitable control on affected systems. The company released software updates that address the issue; for those who cannot yet upgrade, workarounds are provided in the Cisco security advisory. Further updates from Cisco fix multiple denial-of-service (DoS) vulnerabilities in ASA 5500 Series appliances and the Catalyst 6500 Series ASA Services Module (ASASM). Another Protocol Independent Multicast (PIM) DoS hole was closed in the Catalyst 6500 Series Firewall Services Module (FWSM).

Source: <http://www.h-online.com/security/news/item/Cisco-closes-holes-in-its-Security-Appliances-1473257.html>

For more stories, see items [13](#), [30](#), [39](#), and [49](#)

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

49. *March 16, Sanford Herald* – (North Carolina) **Windstream glitch impacts local customers.** A mishap during contract work in northern Lee County left roughly 35,000 Windstream customers in Sanford, Broadway, and the Olivia, North Carolina area without the World Wide Web for hours March 14. A company spokesman said a contractor was boring an underground performing line March 14, when he inadvertently cut a vital fiber line. The mistake cut off Internet in Lee and parts of northern Harnett County over several hours March 14 through March 15.
Source: <http://sanfordherald.com/bookmark/17888038-Windstream-glitch-impacts-local-customers>

For more stories, see items [13](#) and [42](#)

[\[Return to top\]](#)

Commercial Facilities Sector

50. *March 16, WISH 8 Indianapolis* – (Indiana) **Church burns on southwest side.** Firefighters in Wayne Township, Indiana, battled a church fire March 16. The church had significant smoke, fire, and water damage, but no one was injured. No one was inside the building, and firefighters had the fire under control within 30 minutes. Fire officials said they believe the fire was caused by faulty electrical work.
Source: http://www.wishtv.com/dpp/news/local/marion_county/church-burns-on-southwest-side
51. *March 15, Arlington Heights Daily Herald* – (Illinois) **No one injured in Crystal Lake apartments fire.** Fire officials were still investigating a cause for a fire that displaced numerous residents in a Crystal Lake, Illinois apartment complex March 15. No one was seriously injured, however several people were treated at the scene for smoke inhalation and released. The fire caused about \$300,000 in damages. Officials said 26 people were displaced by the fire, smoke, and water damage.
Source: <http://www.dailyherald.com/article/20120315/news/703159852/>
52. *March 15, WOKV 690 AM Jacksonville* – (Florida) **Meth lab investigation at Southside apartment complex.** The Jacksonville, Florida Sheriff's Office and Jacksonville Fire Rescue were on the scene of a possible meth lab at the Woodhollow Apartments, March 15. "During that investigation, they observed chemicals inside an apartment," according to the assistant chief of the Jacksonville Sheriff's Office. "The number of chemicals and the amount of chemicals led them to believe the chemicals are possibly some sort of meth lab." Four units were sealed off, and the apartment management company was working on overnight accommodations for those tenants. One person was arrested in connection to the lab.
Source: <http://www.wokv.com/news/news/meth-lab-investigation-southside-apartment/nLTXF/>

53. *March 15, U.S. Department of Labor* – (New Jersey) **U.S. Labor Department’s OSHA proposes \$121,000 in fines to Dollar Tree Stores for repeat workplace safety hazards at Newark, NJ, store.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) March 15 cited Dollar Tree Stores for two repeat safety violations at its Newark, New Jersey location. The OSHA opened an inspection in response to a complaint alleging blocked fire exits and the unsafe storage of items in stock. Proposed penalties total \$121,000. The first violation was permitting exit routes to be obstructed by boxes and product carts. The second violation was storing materials in an unsafe manner.

Source:

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21984

54. *March 15, Ann Arbor.com* – (Michigan) **Firefighters injured, apartments evacuated as storm blows through Ann Arbor.** Flooding forced the evacuation of an apartment complex in Ann Arbor, Michigan, and several people had to be rescued from cars as streets flooded with up to 4 feet of water in the aftermath of heavy thunderstorms March 15. Residents of the apartment complex were sent to a nearby shelter. Two firefighters also suffered non-life threatening electrical injuries fighting a fire that started when an electrical wire fell onto a garage. The storm was part of a large system that produced a tornado, which touched down in the Dexter area, causing heavy damage.

Source: <http://www.annarbor.com/news/flooded-apartments-evacuated-firefighters-injured-in-ann-arbor/>

For more stories, see items [1](#), [16](#), [25](#), and [40](#)

[\[Return to top\]](#)

National Monuments and Icons Sector

55. *March 16, KJCT 8 Grand Junction* – (Colorado) **Dangerous rock removed from national monument.** Park rangers closed a 4-mile section of Rim Rock Drive in Grand Junction, Colorado, to pull down a potentially dangerous rock from the Colorado National Monument March 15. Crews safely brought down 6 tons of rock. Park rangers first noticed a crack in the rock at the entrance to the upper tunnel on the Fruita side of the monument about 5 years ago. The rock removed will stay in the national monument. The pieces will be placed around the park and used for trail maintenance if needed.

Source: <http://www.kjct8.com/news/30689324/detail.html>

[\[Return to top\]](#)

Dams Sector

56. *March 16, WTHI 10 Terre Haute* – (Indiana) **Bennington levee fix.** Daviess County, Indiana, will be putting up \$1 million to fix two gaping holes in Bennington Levee.

High water along the White River broke through the Bennington Levee last spring and flooded thousands of acres of farm ground. “Of course we have to wait until the ground dries out, but at that point and time it will be July or August,” said the president of the Daviess County commissioners, “but [we are] anticipating this levee being fixed before the end of this summer.” With the spring planting season coming soon, officials and farmers are hoping a big river does not come down the White again this year. “If we get a big river, yeah, it could hold up everything for another season,” said the president. The county has filed a lawsuit against a land owner, farmer, and construction company in connection with the breaks but that case is just beginning.

Source: http://www.wthitv.com/dpp/news/local/southern_indiana/bennington-levee-fix

57. *March 15, KFYP 5 Bismarck* – (North Dakota) **Corps looks to improve Williston levees.** The U.S. Army Corps of Engineers is planning a \$20 million upgrade for improving the 50-year old Williston, North Dakota levee system this summer. They are starting with upgrading 16 pressure relief wells, which are 70 to 100 feet deep and relieve pressure. “The levee system functioned very well during this last event, however the levee system is aging and we just need to upgrade,” said a Corps official. The Corps is also resurfacing the levee and adding more soil to improve the slope. This work will be done for all 9.2 miles of the levee system. The bulk of the project will take place from Mid-May through the fall. At that time the Corps is requesting the public not use the levee system.

Source: http://www.kfyrtv.com/News_Stories.asp?news=55837

58. *March 15, Boise Weekly* – (Idaho) **Civil engineers issue dismal report card for Gem State.** The American Society of Civil Engineers (ASCE) March 15 released their first report card on Idaho’s infrastructure, assessing the status of highways, bridges, dams, wastewater, and more. Out of 11 categories, Idaho scored no better than a B-minus (on wastewater), and at worst a D-minus (for passenger rail). The average grade for Idaho’s infrastructure was a C. The grades were compiled by looking at many different criteria, including condition, maintenance, age, and others. “By 2015, the average age of Idaho’s bridges will be 50 years old, which is the design life on many of these bridges. Many Idaho dams are more than 50 years old,” said the chairman of the 21-member ASCE committee that conducted the study, which is available at <http://sections.asce.org/sis/ReportCard/index.html>.

Source: <http://www.boiseweekly.com/CityDesk/archives/2012/03/15/civil-engineers-issue-dismal-report-card-for-gem-state>

59. *March 15, Fort Lauderdale Sun-Sentinel* – (Florida) **South Florida gets federal deadline to fix failing levee.** February triggered the start of the South Florida Water Management District’s 2-year window to fix the Broward section of the East Coast Protective Levee, which falls short of federal safety standards. The district, Broward County, and eight western cities now have 3 months to finalize an agreement aimed at getting the levee up to the standards of the Federal Emergency Management Agency (FEMA). Inspectors have also identified deficiencies in the Palm Beach County portion of the levee, which will be subject to its own FEMA review. While the water management district acknowledges the need to address the federal concerns over the levee, it contends that the 60-year-old structure still is capable of protecting South

Florida from flooding. The district expects to spend about \$13 million refurbishing the 38-mile long Broward section of the levee.

Source: <http://www.sun-sentinel.com/news/palm-beach/fl-levee-fix-update-20120315,0,5461367.story>

60. *March 15, Omaha World-Herald* – (National) **Corps: Don't get complacent.** Officials from the U.S. Army Corps of Engineers met March 15 with the governor in South Dakota's state capitol to update him on the status of the Corps' post-flood damage studies and dam and structure repairs. The Corps is leading a delegation of engineers and others touring the river's six big dams from Montana to Nebraska the week of March 12 as the Corps moves on from completed critical levee and dam repairs to launching an estimated \$186.3 million in continued work. South Dakota's governor pressed Corps officials to develop a more comprehensive method of determining the amount of snow in the northern Plains and its likely impact on spring runoff into the reservoir system and, eventually, downstream past Omaha and beyond.

Source: <http://www.omaha.com/article/20120315/NEWS01/703159914#corps-don-t-get-complacent>

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: <http://www.dhs.gov/iaipdailyreport>

Contact Information

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

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

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.