Homeland Security

Daily Open Source Infrastructure Report for 2 March 2011

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

For information, click here: http://www.dhs.gov

Top Stories

- Bloomberg reports Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers more than 1 year ago, according to a cyber-security company working for the bank. (See item **13**)
- According to Associated Press, a man armed with an assault rifle, handgun, and a knife walked into the Grant Parish Sheriff's Office in Colfax, Louisiana, took a hostage, and wounded a deputy before being shot. (See item **31**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *March 1, Pueblo Chieftan* – (Colorado) **Outage hits thousands.** About 25,000 Black Hills Energy customers in Pueblo, Colorado were without power February 28 because of technical problems that started at a single substation and quickly caused total outages at six of the substations, according to a company spokesman. St. Mary-Corwin Medical Center was among the customers affected, but the hospital's emergency backup system

switched on "almost instantaneously" and patient safety was not impacted, the hospital CEO said. "We were doing some switching at the Overton substation and the switch that was being opened didn't open properly and, consequently, we had a failure. It resulted in an outage that affected about 25,000 customers. We lost six of our substations for between 12 and 15 minutes," a company spokesman said. The outage affected customers in Belmont, Blende, the St. Charles Mesa and east to the Pueblo Chemical Depot, and a portion of Pueblo's South Side neighborhood along Prairie Avenue and the hospital.
Source: http://www.chieftain.com/news/local/outage-hits-thousands/article_3ce7cac8-43be-11e0-bcf3-001cc4c002e0.html

2. *March 1, RiverheadLOCAL.com* – (New York) **21,000 worth of copper wire reported stolen at EPCAL one day after substation vault fire.** The theft of $21,000 worth of copper wire at the Calverton Enterprise Park (EPCAL) in Riverhead, New York, was reported to Riverhead Town Police February 25, 1 day after an underground fire at the Long Island Power Authority substation at the site cut power to the entire industrial park. The theft occurred between December 1, 2010 and February 25, when a site manager discovered it, the police report said. Thieves made off with about 1,000 feet of copper wire, taken from within an above-ground outside conduit that ran from a service panel off Scott Avenue to an office trailer, police said. The lock to the trailer was also cut, and a $100 tool box was stolen. Police said the perpetrator(s) accessed the property, which is surrounded by a chain-link fence, by cutting a hole in the fence. There was no alarm or surveillance system on the property, according to the police report. The site is one of several at EPCAL still owned by the U.S. Navy, which retained certain parcels on the former Grumman site for environmental remediation subsequent to transferring 2,900 acres to the Town of Riverhead in 1998.
Source: http://www.riverheadlocal.com/local-news-content/1715-major-copper-wire-theft-at-epcal

3. *March 1, Fayetteville Observer* – (North Carolina) **Raeford highway reopens after tanker truck wreck.** U.S. 401 east of Raeford, North Carolina, reopened the morning of March 1 after emergency workers spent the night burning propane from a wrecked tanker truck. The driver of that truck is in critical condition at UNC Hospitals, a spokesman there said. The highway was closed between North Parker Church, Johnson Mill and Scull roads February 28 after a propane tanker and a pickup truck collided. The 2,200-gallon tanker was traveling toward Raeford when a Chevrolet pickup truck turned left in front of it. The impact sent both vehicles off the road and the tanker overturned, a patrolman said. Authorities determined the tanker was too badly damaged to transfer the propane to another truck, so they opted to burn off the gas, according to the Hoke County Emergency Management director.
Source: http://www.fayobserver.com/articles/2011/03/01/1074912?sac=Home

4. *March 1, KBTX 3 Bryan/College Station* – (Texas) **Texas City gas pipeline leak repaired.** A gasoline pipeline break in Southeast Texas has been repaired and cleanup continues after about 5,000 gallons leaked into a bayou. The Galveston County Daily News reported the pipeline owner, Magellan Midstream Partners, received approval from the state to put the Texas City line back into service February 28. No injuries were

reported February 24 when the break forced the evacuation of more than 30 homes and businesses. The spill forced the rerouting of some traffic. A company spokesman said a boom between a drainage canal and the bayou remains in place, as a precaution.
Source: http://www.kbtx.com/state/headlines/Texas_City_Gas_Pipeline_Leak_Repaired_117151943.html

5. *February 28, Associated Press* – (West Virginia) **Massey subsidiary security chief indicted in West Virginia mine explosion.** The security chief of a Massey Energy Co. subsidiary was charged in a federal indictment with obstructing the investigation of a 2010 explosion that killed 29 miners at the company's Upper Big Branch Mine in Montcoal, West Virginia, federal prosecutors said February 28. The indictment accuses the security chief of lying to an FBI agent and a federal Mine Safety and Health Administration (MSHA) inspector. It also charges he ordered an employee to dispose of thousands of pages of security documents from the Raleigh County mine more than 9 months after the explosion. The indictment said Massey regularly violated federal law by warning underground workers when government officials arrived to conduct safety inspections at its mines. The father of one of the victims told a congressional panel last May that Massey used radio messages warning that "a man" was on the property when MSHA arrived for an inspection. The security chief is accused of lying when he told FBI and MSHA investigators January 21 that company policy prohibited such warnings.
Source: http://www2.newsvirginian.com/news/2011/feb/28/5/massey-subsidiary-security-chief-indicted-west-vir-ar-873340/

6. *February 28, KOMO 4 Seattle* – (Washington) **Natural gas compressor explodes outside Pierce Transit building.** A natural gas explosion outside the Pierce Transit administration building in Lakewood, Washington, ignited flames and released big plumes of smoke seen for miles February 28. Firefighters arrived at the building on South Tacoma Way at 96th Street just after 5 p.m. to find a natural gas compressor on fire, said the West Pierce Fire and Rescue captain. The compressor was located at a refueling island in the building's lot. Officials ordered an evacuation of buildings within a quarter-mile radius of the explosion site as a precaution, but roads were reopen after Puget Sound Energy shut off the gas line around 6 p.m. One witness said he heard and felt three consecutive explosions from about a mile away. Investigators are working to determine what caused the compressor to explode. No one was injured.
Source: http://www.seattlepi.com/local/436246_gas28.html

For another story, see item **49**

[Return to top]

Chemical Industry Sector

7. *March 1, Spencer Daily Reporter* – (Iowa) **Accident releases anhydrous, closes B-17.** A traffic accident February 28, resulted in the closure of Clay County Road B-17 (300th Street), about 4 miles east of Langdon, Iowa. The road remained closed March

1, and the Clay County sheriff anticipated it might remain impassable until midnight depending on the amount of cleanup required. The cause of the accident remains under investigation. Details from the scene — near the 290th Avenue intersection — in northern Clay County, suggest a tanker truck hauling anhydrous ammonia left the traveled portion of the roadway on the curve near Dan Green Slough. The tractor and tanker separated at some point, leaving the tanker sitting in a field about 200 feet south of the roadway, spraying anhydrous fumes into the air. Initially the smell was reported as far as 2 miles away. Emergency responders from the Dickens, Fostoria, and Spencer fire departments, along with the Clay County Sheriff's Office and Iowa State Patrol, closed off roadways to traffic about 1 mile away from the scene in each direction. The driver of the truck was transported to a hospital. The sheriff said before the scene could be cleared, a crane from Sioux Falls would be brought in, and tankers would be needed to off-load the remaining fluid in the tanker. Clay County Emergency Management and Iowa Great Lakes Chapter of the Red Cross assisted.
Source: http://www.spencerdailyreporter.com/story/1706950.html

8. *March 1, Charleston Daily Mail* – (West Virginia) **DuPont reports ammonia leak at Belle plant.** DuPont said about 20 pounds of ammonia apparently leaked from the top of the ammonia tank at its Belle, West Virginia, plant March 1. The plant sounded the fume alert at 2:36 a.m. "after a remote sensor detected a small leak from a vent on top of the ammonia tank," DuPont said in a statement. "The plant emergency response team responded and closed the valve from the tank leading to the vent. No one was injured during the incident," the company said. "The Belle Fire Department responded to the plant gate as a precaution per our normal joint protocol. The all clear was sounded at 3:12 a.m," the statement continued. "Our initial calculations indicate that the quantity released was approximately 20 pounds, which is below the reportable threshold quantity. We are continuing our investigation to finalize our calculations on the quantity released and determine the cause of the leak," DuPont said. "All appropriate government agencies have been notified."
Source: http://www.dailymail.com/News/Kanawha/201103010464

For another story, see item **24**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

9. *March 1, Associated Press* – (Virginia) **Dominion says nuclear plans at Virginia plant remain unchanged despite partner's withdrawal.** Energy company Dominion said it has not changed its plans on a potential third nuclear reactor at its North Anna Power Station in Mineral, Virginia despite a partner's decision to withdraw from the project. Richmond-based Dominion said February 28 that Old Dominion Electric Cooperative has decided to pull out of the project. The wholesale power supplier owns an 11.6 percent share in Dominion's two current nuclear units at the Louisa County plant and had been a partner in the development of a proposed third unit. The Nuclear Regulatory Commission (NRC) is currently reviewing Dominion's application to build and operate the new reactor, but the company has not yet made a decision on when and

if it will build it.
Source: http://www.wtkr.com/news/sns-ap-va--dominion-nuclearplans,0,5668620.story

10. *February 27, Associated Press* – (New York) **Indian Point Unit 3 reactor back online after repairs.** Service has been restored to a reactor at the Indian Point nuclear power plant in Buchanan, New York after it was shut down to undergo repairs. Indian Point's Unit 3 was back online February 25 after workers patched a pipe that delivers water to cool the reactor. Nuclear Regulatory Commission (NRC) officials said no radioactive material was released. It was shut down February 22 after workers noticed a water leak.
Source: http://www.recordonline.com/apps/pbcs.dll/article?AID=/20110227/NEWS/110229808/-1/SITEMAP

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

11. *February 28, Computerworld* – (International) **NASA: Robotic work station fails during spacewalk.** The central command post for the International Space Station's robotics work failed February 28 during the first spacewalk of the shuttle Discovery's final space mission. Two NASA astronauts had just completed the first task of the spacewalk when the robotic work station in the space station's new seven-window cupola stopped working, according to NASA. Two other astronauts had been running the station's robotic arm to help the spacewalkers install an extension to a power cable. Instead of waiting about 30 minutes to reboot the work station in the new cupola, the astronauts manning the robotic arm switched to a different robotic work station inside the space station. The spacewalkers will need the robotic arm as they work to move an 800-pound failed pump module to an external platform where it will wait for a ride back to Earth on another mission.
Source: http://www.computerworld.com/s/article/9211880/NASA_Robotic_work_station_fails_during_spacewalk

12. *February 28, DefenseNews* – (National) **Company plans fixes for JSF helmet display issues.** Fixes are in the works for several technical glitches that have been plaguing the helmet-mounted display in F-35 fighter jets, said an official from Vision Systems International, which builds the unit. Among the problems pilots have complained of are latency — where the imagery does not keep up with the motion of the pilots head, imagery that is misaligned with the pilot's vision, and jittery images. The problem is especially pronounced with the helmet's night-vision system, which is meant to display

images from six infrared cameras mounted around the aircraft's fuselage, the Joint Strike Fighter program chief said. The program has been looking at alternative night-vision systems for the first training unit, scheduled to receive its first F-35s in May. The program chief said near-term fixes could include moving the imagery to the aircraft's head-down flat-panel displays, and having pilots use conventional night-vision goggles. But these are not satisfactory long-term solutions, he said. The president of Vision Systems International said the company has long-term solutions mapped out.
Source: http://www.defensenews.com/story.php?i=5828022&c=AME&s=AIR

[Return to top]

Banking and Finance Sector

13. *February 28, Bloomberg* – (International) **Morgan Stanley attacked by China-based hackers who hit Google.** Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers more than 1 year ago, according to e-mails stolen from a cyber-security company working for the bank. The e-mails from the Sacramento, California-based computer security firm HBGary Inc., which identify the first financial institution targeted in the series of attacks, said the bank considered details of the intrusion a closely guarded secret. "They were hit hard by the real Aurora attacks (not the crap in the news)," wrote a senior security engineer at HBGary, who said he read an internal Morgan Stanley report detailing the so-called Operation Aurora attacks. The nickname came from McAfee Inc., a cyber-security firm, which said the attacks occurred for about 6 months starting in June 2009 and marked "a watershed moment in cyber security." The number of companies known to be hit in the attacks was initially estimated at 20 to 30 and now exceeds 200, said the senior vice president for Terremark Worldwide Inc., which provides information-technology security services. The HBGary e-mails do not indicate what information may have been stolen from Morgan Stanley's databanks or which of the world's largest merger adviser's multinational operations were targeted.
Source: http://www.bloomberg.com/news/2011-02-28/morgan-stanley-network-hacked-in-same-china-based-attacks-that-hit-google.html

14. *February 28, Cypress Times* – (International) **Alleged supporter of terrorist group extradited from Paraguay.** Following a joint investigation by U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) and the FBI, a former resident of Brooklyn, New York, has been charged with conspiring to provide material support to Hizballah. The 38-year-old is a dual citizen of the United States and Lebanon. The suspect is among several defendants charged in the conspiracy. He was indicted November 24, 2009, along with nine co-defendants. The suspect was taken into U.S. custody in Asuncion, Paraguay February 24 by U.S. Marshals who escorted him to Washington D.C. At the time of the indictment, the suspect had left the United States. On June 15, 2010, Paraguayan authorities arrested him for material support of terrorism. He is charged in 28 of 31 counts in the indictment, including conspiring to provide material support to Hizballah in the form of proceeds from the sale of counterfeit money, stolen (genuine) money, and fraudulent passports. According to the indictment, the suspect and several other defendants were also charged with several

counts of transporting stolen goods, trafficking in counterfeit goods, and making false statements to government officials.
Source:
http://www.thecypresstimes.com/article/News/National_News/ALLEGED_SUPPORTER_OF_TERRORIST_GROUP_EXTRADITED_FROM_PARAGUAY/41183

15. *February 26, Federal Bureau of Investigation* – (New Jersey) **Mortgage company president sentenced for orchestrating $136 million fraud scheme.** A Montclair, New Jersey, man was sentenced February 26 to 168 months in prison for his role in orchestrating the $136 million fraud scheme that bankrupted Pine Brook, New Jersey-based United States Mortgage Corp. and its subsidiary, CU National Mortgage, LLC, the U.S. attorney announced. The 47-year-old man, the former president and controlling shareholder of United States Mortgage, previously pleaded guilty before a U.S. district judge to one count of mail and wire fraud conspiracy and one count of money laundering. The judge also imposed the sentence February 26 in Newark federal court. According to documents filed in this and related cases and statements made in court: Beginning as early as 2002 to January 27, 2009, the man conspired to fraudulently sell Fannie Mae hundreds of loans belonging to various credit unions. Other members of the conspiracy included United States Mortgage's chief financial officer (CFO) and its servicing manager. The lead conspirator directed the former CFO, who provided numerous reports to credit unions falsely stating loans that had been sold were still in the credit unions' portfolios, to falsify records to conceal the fraudulent sales. The lead conspirator admitted he devised the scheme to prop up United States Mortgage, and that he used the proceeds to fund United States Mortgage's operations, his personal investments, and investments he made on United States Mortgage's behalf.
Source:
http://7thspace.com/headlines/374063/mortgage_company_president_sentenced_for_orchestrating_136_million_fraud_scheme__.html

For another story, see item **43**

[Return to top]

Transportation Sector

16. *March 1, Associated Press* – (Connecticut) **Nose gear on plane at Conn. airport collapses.** Passengers were evacuated from a plane at Bradley International Airport in Windsor Locks, Connecticut, March 1 when the nose gear of their aircraft collapsed as it was pushing away from the gate. A spokeswoman for the Federal Aviation Administration said 29 passengers and three crew members were taken off the Embraer 145 operated by Trans States Airlines, a contractor for US Airways, after the front landing gear on the Pittsburgh-bound flight collapsed at about 6:45 a.m. A US Airways spokeswoman said the cause of the collapse remains under investigation. Passengers were placed on other flights.
Source: http://www.wggb.com/Global/story.asp?S=14161306

17. *March 1, Mansfield News Journal* – (Ohio) **Flooding leads to evacuation of 80 Morrow County residents.** Morrow County commissioners in Ohio declared a state of flood emergency at 9:47 a.m. March 1 as emergency personnel were evacuating trailer courts, an apartment complex, and the Morrow County dog shelter, the commissioner said. About 4:15 p.m. February 28, the director for Morrow County emergency management, said Morrow County had 28 road closings, including five state routes. Some of those have major culverts washed out, "so they'll be down for a minimum of a week," he said.
Source:
http://www.mansfieldnewsjournal.com/article/20110301/NEWS01/103010318/Flooding-leads-evacuation-80-Morrow-County-residents?odyssey=tab|topnews|text|Frontpage

18. *February 28, Corpus Christi International Airport* – (Texas) **International airport to hold emergency exercise.** The Corpus Christi International Airport (CCIA) in Corpus Christi, Texas will conduct a full-scale Aircraft Emergency Exercise involving dozens of local, state, and federal agencies. The exercise will begin at 9 a.m. March 3 near the new airport maintenance facility. The drill is part of CCIA's Triennial Exercise, which is required by the Federal Aviation Administration (FAA) as a way to evaluate the effectiveness of the Airport's Emergency Plan. This year's scenario for the simulated emergency involves a regional jet carrying approximately 50 passengers. Agencies taking part in the exercise include the American Red Cross, United States Customs and Border Protection, Del Mar College, Corpus Christi Police Department, Corpus Christi Fire Department, United States Coast Guard, Texas Department of Public Safety, Transportation Security Administration, Civil Air Patrol, Naval Air Station Corpus Christi Fire Department, FAA, Nueces County Sheriff's Department, Christus Spohn Health System, and others.
Source: http://www.kristv.com/news/international-airport-to-hold-emergency-exercise/

19. *February 28, Florida Today and Daytona Beach News-Journal* – (Florida) **Fire prompts voluntary evacuation, shutdown of U.S. 1.** A fast-moving brush fire in north Brevard, Florida, February 28 prompted officials to call for a voluntary evacuation of residents who live in the area bordered by County Road 5A on the north, State Road 46 on the south, U.S. 1 on the east, and the St. Johns River on the west. Interstate 95 was closed in both directions from State Road 46 (Mile Marker 223) in Mims north to State Road 442 (MM 244). U.S. 1 had previously been closed from SR 46 to Maytown Road in Volusia County. The fire jumped I-95 between 4 and 5 p.m. February 28, according to a wildfire mitigation specialist for the state division of forestry. Reports said flames that reached 20 feet tall were blown east by strong winds. The fire had jumped a portion of U.S. 1 by 9:30 p.m. February 28.
Source:
http://www.floridatoday.com/article/20110228/BREAKINGNEWS/110228018/Fire-prompts-shutdown-95-U-S-1?odyssey=tab|topnews|text|Local News

For more stories, see items **3**, **6**, **7**, **24**, and **28**

[Return to top]

Postal and Shipping Sector

20. *March 1, WHIO 7 Dayton* – (Ohio) **Greene County career center evacuated.** The Dayton Bomb Squad was called February 28 to the Greene County Career Center in Ohio to investigate a suspicious package. Strange labeling and addressing on a package that arrived in the mail alerted faculty who called the Greene County Sheriff's Office around 4 p.m., the Greene County Sheriff's Office said. The building was evacuated in an orderly fashion, and evening classes were canceled. Between 60 and 80 people were affected by the cancellations. The sheriff's office called the Dayton Bomb Squad to check the package. They later detonated the box and determined that it contained t-shirts and no dangerous items or substances. Classes at the career center were scheduled to resume March 1.
Source: http://www.whiotv.com/news/27031194/detail.html

[Return to top]

Agriculture and Food Sector

21. *March 1, Reading Eagle* – (Pennsylvania) **Birds apparently poisoned by local farmer, state says.** Dozens of birds found dead along a highway in Spring Township, Pennsylvania, February 27 apparently were legally poisoned by a local farmer, the Pennsylvania Game Commission said February 28. Motorists that day spotted the European starlings dead on or along Route 222 just north of Route 724. Game Commission officials said there were at least 100 carcasses. The commission tested some of the birds and found they were killed by Starlicide, a poison designed specifically for European starlings but less toxic to most other birds and mammals, a commission spokeswoman said. Because the United States Department of Agriculture (USDA) considers the European starling an invasive species and a pest to farmers, the department sets out Starlicide for them in areas where they are especially problematic, a spokeswoman said. Farmers are allowed to do likewise because the birds eat large amounts of livestock feed, fruit and grain, and their feces damages equipment, according to the USDA.
Source: http://readingeagle.com/Article.aspx?id=290815

22. *February 28, U.S. Food Safety and Inspection Service* – (National) **California firm recalls chicken and mushroom pie products due to mislabeling and undeclared allergen.** Piccadilly Fine Foods, a Santa Clara, California establishment, recalled about 775 pounds of chicken and mushroom pie products because they may contain an undeclared allergen, egg, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced February 28. The following products are subject to recall: 12-pound cases of "Piccadilly Fine Foods Chicken and Mushroom Pastie" with each case containing 24 individual packages. The chicken-and-mushroom pies were produced on various dates between August 1, 2010 and February 25, 2011. But some products subject to recall during this time frame are correctly labeled in that they do include "egg" in the ingredient statement. The products were shipped to distributors in California, Colorado, Florida, and Texas for further distribution to retail outlets.

Source:
http://www.fsis.usda.gov/News_&_Events/Recall_015_2011_Release/index.asp

[Return to top]

Water Sector

23. *February 28, U.S. Environmental Protection Agency* – (Alaska) **Alaska placer miner settles EPA Clean Water Act discharge violations.** A Trapper Creek, Alaska, resident agreed to pay the U.S. Environmental Protection Agency (EPA) a $8,000 penalty to resolve a Clean Water Act violation at his placer mine, near Petersville, Alaska. His agreement with EPA, called a Consent Agreement and Final Order covers a violation at a placer mine he operated along Spruce and Cache Creeks in the Yentna Mining District. During an overflight of the man's placer mining operations in July 2010, inspectors documented the operator's failure to retain wash plant wastewaters, which were allowed to enter a ditch that was directly connected to Spruce Creek.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/5D467C2273B76C2A852578450075750D

24. *February 28, Pacific News Center and Guam News* – (Guam) **Chlorine leak prompts evacuation of Two Lovers Point area;** A chlorine leak at the Northern Wastewater Treatment Plant in Guam prompted an evacuation from the plant February 28, as well as from the Two Lovers Point area, the Ukudu Village, and the Tanguiessen Beach area. A statement from Guam Homeland Security stated the quantity of the leakage is "minimal." A 1-ton chlorine cylinder tank containing 500 pounds of liquid chlorine leaked. The statement said the leakage was high enough to cause discomfort, but not a serious health threat. However, Guam Water Authority's (GWA) safety manager issued a statement saying "we are not taking any chances of exposing anyone." The area around Two Lovers Point will remain closed for 24 to 26 hours. The leak was first reported around 10 a.m. Guam fire and police departments responded to the scene and evacuated the area. Police set up road blocks along all the roads leading into the area and they turned away all vehicles that approached the site. The fire captain said the leak was detected by instruments at the sewer plant. A team of off-island specialists hired by GWA's contractor Violia Water, have been working to drain 11 old chlorine tanks discovered by Violia behind the treatment plant. There are no residential homes in the immediate area.
Source:
http://www.pacificnewscenter.com/index.php?option=com_content&view=article&id=11909:chlorine-leak-prompts-evacuation-at-northern-wastewater-treatment-plant&catid=45:guam-news&Itemid=156

25. *February 28, Tulsa World* – (Oklahoma) **Okmulgee to revamp water treatment plant.** A $10 million revamping of Okmulgee's water treatment plant in Okmulgee, Oklahoma will begin next month and will eventually bring the water system in compliance with federal regulations, officials said. The system became non-compliant in 2005 after the U.S. Environmental Protection Agency set new limits for various contaminants, city officials said. The city violated a drinking water standard by having

excessive levels of trihalomethane, a chlorine disinfectent byproduct. Work on the treatment plant, located on Oklahoma 56 about 1 mile west of Okmulgee, should start March 15 and take 15 months to complete, city officials said.
Source: http://www.tulsaworld.com/news/article.aspx?subjectid=11&articleid=20110228_12_A4_OKMULG324935

26. *March 1, Monterey County Herald* – (California) **Wastewater accidentally discharged.** A chain of equipment and alarm failures sent about 300,000 gallons of partially treated wastewater into Carmel Bay for about 4 hours February 27 in Monterey, California. The wastewater had gone through all treatment stages at the Carmel Area Wastewater District's plant except for the final disinfection step of chlorine injection, the district manager said. District and county health officials took water samples February 28 for coliform bacteria levels. "We don't think the impacts will be major," the manager said. The district contacted county, state and federal officials about the incident and expected to be fined by state and water quality officials for the unauthorized discharge. The incident started about 4:30 p.m. February 27 when the plant's primary disinfection system failed because the equipment pulled away from a wall to which it was bolted. Two alarm systems using a pager and a cell phone failed to notify anyone about the problem until 8:15 p.m. About the same time, an on-call plant worker logged on to the system and detected the problem. The district provides wastewater treatment service for Carmel, the Pebble Beach Community Services District, and some customers near the mouth of Carmel Valley. The treated wastewater is discharged about 600 feet offshore.
Source: http://www.montereyherald.com/local/ci_17509001?nclick_check=1

For another story, see item **4**

[Return to top]

Public Health and Healthcare Sector

27. *March 1, WCSC 5 Charleston* – (South Carolina) **Daniel Island medical center roof collapses in fire.** A fire engulfed a Daniel Island medical center in Charleston, South Carolina, causing the roof to collapse March 1. The fire broke out at 899 Island Park Drive around 2:30 a.m. Firefighters first reported seeing flames shooting 30 to 40 feet high from the building. After the fire was put out, firefighters remained on the scene to make sure hot spots would not re-ignite the structure. Five different Charleston area fire departments responded. No one was injured in the fire. The building housed Parkwood Pediatric Group and Crescent Moon Orthodontist. Firefighters are investigating the cause of the fire.
Source: http://www.live5news.com/Global/story.asp?S=14160315

28. *February 28, Washington Post* – (National) **D.C. Health Department issues measles alert.** A woman infected with measles traveled through Washington, D.C. and Maryland after flying into Dulles International Airport in Dulles, Virginia, it was disclosed February 28. The 27-year-old New Mexico resident landed at the airport

February 20 and left the region February 22, from Baltimore-Washington International Marshall Airport (BWI) in Baltimore, Maryland. D.C. Health Department officials said she spent time in Washington, D.C. during this period, apparently in Georgetown and Columbia Heights. The department said between 10:30 a.m. and 2:30 p.m. February 21, the woman went from Georgetown to Columbia Heights, using buses on the D1 or D6 route for part of the trip. She apparently returned between 1:30 p.m. and 5:30 p.m. on an S2 or S4 bus, the health department said. In Columbia Heights, she might have been at the Potbelly Sandwich Shop in the 1400 block of Irving Street NW. The medical director of the public health division of the New Mexico Health Department said the woman apparently was exposed to measles while in Europe. She flew from BWI to Denver, and then to Albuquerque.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/02/28/AR2011022806618.html?hpid=newswell

For another story, see item **1**

[Return to top]

Government Facilities Sector

29. *February 28, KPRC 2 Houston* – (Texas) **Fake bomb found at Houston City Hall.** A fake bomb made to look like the real thing was found February 28 outside the city hall in Houston, Texas, police said. The city hall was evacuated after a suspicious package was found about 7:15 a.m. Each entrance to the building was lined with crime scene tape. Houston police said a security guard spotted the large duffel bag, which contained a rolled-up magazine stuffed with glass, metal, and wires that had been wrapped in duct tape. The bomb squad X-rayed the package and then remotely detonated the item shortly before 8:30 a.m. Detectives are working to determine who left the package and who made it. Several dozen people were standing outside city hall. The city's mayor had not yet arrived at city hall when the package was found.
Source: http://www.click2houston.com/news/27022733/detail.html

30. *February 28, New Philadelphia Times Reporter* – (Ohio) **No bomb found after latest Stark State threat.** For the fourth time since January 24, a bomb threat shut down Stark State College in Jackson Township, Ohio, for part of the day February 28. The latest threat was made around 12:07 p.m. February 28, forcing the evacuation of the main campus and closing satellite centers. No explosive devices were found. The campus was set to reopen at 5 p.m. for evening classes. According to the Jackson Township Police Department, an unidentified man telephoned the main switchboard at Stark State saying there was a bomb on the campus. Students, faculty, and staff were notified via text messages around 12:30 p.m. that the campus was closed due to the threat. Stark State and its satellite centers stayed closed until officials were given the all-clear to reopen. Jackson Township police were assisted by specially trained dogs from the Summit County Sheriff's Office, Canton police, and the University of Akron. Campus security personnel also helped in the investigation.
Source: http://www.timesreporter.com/communities/stark/x2114547345/Stark-State-College-closed-by-another-bomb-threat

For more stories, see items **1**, **20**, **32**, and **44**

[Return to top]

Emergency Services Sector

31. *March 1, Associated Press* – (Louisiana) **Louisiana deputy shot in sheriff's office.** A man armed with an assault rifle, handgun, and a knife walked into the Grant Parish Sheriff's Office in Colfax, Louisiana February 28, took a hostage, and wounded a deputy before being shot. The suspect had the weapons plus extra magazines and ammunition for each firearm when he walked into the sheriff's office at 3 p.m., state police said. After he started shooting, deputies in the building returned fire. The gunman, a 52-year-old man from Colfax, Louisiana, and the deputy were in the hospital, a state police trooper said in a news release. The suspect is listed in critical but stable condition and the deputy was listed as stable, state police said. It is unknown if the deputy was the hostage. A spokesman said since it was an ongoing investigation that he would not release more details on what happened. Police did not release a motive.
Source: http://officer.com/online/article.jsp?siteSection=1&id=57051

32. *March 1, WFED 1500 AM Washington D.C.* – (National) **DHS to gain real-time access to DoD biometrics.** The Department of Homeland Security (DHS) hopes to soon have real-time access to the military's biometrics database letting them better sort out who's who at U.S. points of entry. The capability will be similar to what DHS is already doing with the FBI, and through it, local law enforcement agencies around the country said the director of DHS's U.S. VISIT program. U.S. VISIT, the office responsible for screening foreign visitors to the U.S.-is the main repository for DHS' biometric data. That information, mainly fingerprint data, can be shared between DHS and the criminal record system that the FBI holds at its Criminal Justice Information Services division in West Virginia. The director said DHS had already proven the value of biometric information sharing through the Secure Communities program, which lets participating local law enforcement see data held in Homeland Security databases. He said that data comes in handy when law officers encounter a suspect who gives a false name. Since DHS also has access to biometric data held by the FBI, its Customs and Border Protection agents can make better decisions about who to let into the country. "Prior to a pilot in Detroit that we will now expand to other locations, we had people coming into the country with criminal history that made them ineligible to come into the country," the director said. "But they came into the country because we didn't know about it. We can now search the FBI's criminal master file-65 million prints-in under 15 seconds. That is a tremendous, tremendous step forward in both the idea of leveraging information sharing and the technical interoperability between the two systems."
Source: http://www.federalnewsradio.com/?nid=35&sid=2289626

33. *February 28, Escondido North County Times* – (California) **San Marcos: Sheriff's station evacuated after person turns in old grenade.** Authorities evacuated the front portion of the San Marcos station of the San Diego, California county sheriff's

department February 28 after a person tried to turn in what ended up being an inert World War II-era grenade, sheriff's officials said. The sheriff's bomb and arson squad was called to the station about 2:30 p.m. to take possession of the ordnance, which was in the parking lot of the station, a sheriff's department lieutenant said. The person who brought the grenade to the station, north of Highway 78, had no ill intent, but was simply trying to turn in the potentially dangerous item to authorities, officials said. A police lieutenant stated the evacuation lasted about an hour.
Source: http://www.nctimes.com/news/local/san-marcos/article_263084d6-439c-11e0-b2ed-001cc4c03286.html

34. *February 28, WRTV 6 Indianapolis* – (Indiana) **Critical upgrade to Indy emergency system shelved.** Plans to overhaul a critical tool used by Indianapolis, Indiana emergency crews in time for the 2012 Super Bowl have been shelved. The city has received millions of dollars in federal funding to upgrade or replace its aging enhanced Computer Aided Dispatch system, or CAD, which allows police and firefighters to communicate with 911 operators. But the current system, put in place in 1999, is quickly becoming obsolete and is one of only a few still being used across the country. Millions of dollars in federal funding have been secured for the upgrade. Based on information from the consultant hired for the project, bids should have gone out last October to get the project completed in time for the Super Bowl. Despite numerous requests for information February 28, no one within city government could explain why the project was being shelved. The new CAD could cost anywhere from $8 million to $20 million with enhanced features. Sources said the funding expires in 2012.
Source: http://www.theindychannel.com/news/27029488/detail.html

35. *February 28, Orlando Sentinel* – (Florida) **Prankster uses deputy's stolen radio to report 'officer down'.** A portable radio stolen from a Lake County deputy sheriff in Tavares, Florida, was used to make false reports February 28 about an officer being shot, authorities said. Lake County officials tried unsuccessfully to pinpoint the prankster's location using the radio's global positioning system. When they surveyed the crime scene, Sumter detectives found footprints on the officer's driveway that read "Reebok." A sheriff's office bloodhound caught a scent, but the track went cold. Similar prints were found at another home, deputies said. The neighbor reported approaching three young men earlier and gave authorities a description of one of the men. "We are following up a number of leads, but we plan to make an arrest soon," a Sumter County sheriff's office lieutenant said. The man or men involved will face burglary, grand theft, and unlawful-communication charges. The deputy's radio is valued at about $4,100.
Source: http://www.orlandosentinel.com/news/crime/os-stolen-deputy-radio-chaos-lake-20110228,0,4956688.story

36. *February 26, Palm Springs Desert Sun* – (California) **Local man taken into custody for death threats against FBI.** A Cathedral City, California man accused of making death threats against an FBI agent was ordered February 25 to be placed in a residential substance abuse facility pending another court hearing in March, according to a U.S Attorney's Office. The suspect was taken into custody February 24 on suspicion of threatening, in a telephone message, to kill an FBI agent and could face up to 10 years

in prison if convicted an FBI spokeswoman said. He was indicted by a federal grand jury and made his initial court appearance February 24 at the Riverside, California federal courthouse on one count of threatening a federal law enforcement officer. He could have been ordered to remain in custody without bail during the February 25 detention hearing, but instead was sent to the substance abuse facility, according to the U.S. attorney's office.
Source: http://www.mydesert.com/article/20110226/NEWS0802/102260307/Local-man-taken-into-custody-death-threats-against-FBI?odyssey=mod|newswell|text|Frontpage|s

For another story, see item **18**

[Return to top]

Information Technology Sector

37. *March 1, Help Net Security* – (International) **Reset Gmail accounts to be restored completely.** Gmail users that managed to enter their accounts only to find them devoid of any content can find relief, as Google said things will be back to normal for all affected users very soon. According to Google, the bug that triggered the event managed to affect many copies of the data in multiple data centers, but the information has also been backed up on tapes which have not been affected since they are offline. "But restoring data from them also takes longer than transferring your requests to another data center, which is why it's taken us hours to get the email back instead of milliseconds," explained Google. It blamed the bug on a storage software update that was being deployed at the time.
Source: http://www.net-security.org/secworld.php?id=10682

38. *March 1, Softpedia* – (International) **LastPass fixes serious cross-site scripting vulnerability.** Password management service LastPass has fixed a serious cross-site scripting vulnerability on its Web site which could have been exploited to obtain sensitive information about other people's accounts. LastPass allows users to generate secure passwords for each of their accounts and store them inside an encrypted container controlled by a master password. The company offers extensions for all major browsers, which help with auto-fill and other operations, but the login details can also be accessed via its Web site. The flaw on lastpass(dot)com was discovered by a United Kingdom independent security researcher who notified the company. The vulnerability, which LastPass said was a reflected cross-site scripting (XSS) one, could have been exploited by loading the vulnerable page in a frame on another Web site. If the victim browsed that site while logged into LastPass, the attacker could have retrieved the e-mail address, password reminder, list of sites, and log-in history. In a post on its official blog, LastPass assured users the vulnerability was fixed before it could be exploited.
Source: http://news.softpedia.com/news/LastPass-Fixes-Serious-Cross-Site-Scripting-Vulnerability-186774.shtml

39. *March 1, H Security* – (International) **19 vulnerabilities - Chrome 9 update proves expensive for Google.** Google has released version 9.0.597.107 of its Chrome browser,

which fixes a total of 19 security vulnerabilities, 16 of them rated as high risk. It was possible to crash the browser using JavaScript dialogues and SVG files, or to use the address bar for URL spoofing. Also fixed is an integer overflow when handling text areas. Google is keeping full details of the vulnerabilities secret until the bulk of users have switched to the new version.
Source: http://www.h-online.com/security/news/item/19-vulnerabilities-Chrome-9-update-proves-expensive-for-Google-1199922.html

40. *March 1, Help Net Security* – (International) **Malware family integration across botnets.** Analysis by Symantec reveals that in February, 1 in 290.1 e-mails (0.345 percent) was malicious making February among the most prolific time periods both in terms of simultaneous attacks and malware family integration across Zeus (aka Zbot), Bredolab, and SpyEye. Also in February, there were at least 40 variants of malware associated with the Bredolab Trojan, accounting for at least 10.3 percent of e-mail-borne malware blocked by MessageLabs Intelligence in February. These latest findings reveal that contrary to recent beliefs, Bredolab is not dead and techniques previously associated with Bredolab malware have now become more common among other major malware families. Since the end of January, MessageLabs Intelligence has tracked significant volumes of collaborative attacks that make use of well-timed and carefully crafted targeted techniques. As February began, the attacks increased in number and these malware families were used aggressively to conduct simultaneous attacks via propagation techniques, signaling the likelihood of a common origin for these infected e-mails.
Source: http://www.net-security.org/malware_news.php?id=1646

41. *February 28, The Register* – (International) **Tainted ads punt scareware to surfers on LSE and Myvue sites.** Several highly trafficked United Kingdom sites – including the Web site of the London Stock Exchange – served malware-tainted ads as the result of a breach of security by a third-party firm they shared in common. Surfers visiting auto-trading site Autotrader(dot)co(dot)uk and the cinema site Myvue(dot)com were also exposed to the attack, which stemmed from a breach at their common ad provider, Unanimis, rather than at any of the three sites themselves. Unconfirmed reports suggest eBay(dot)co(dot)uk was also affected. The malicious ads made several concealed redirects before dropping surfers on a portal soliciting rogue anti-virus (scareware). By attacking third-party networks rather than Web sites, cyber criminals can increase the potency of attacks, according to an official from Websense Security Labs.
Source: http://www.theregister.co.uk/2011/02/28/tainted_ads_blight_uk_sites/

42. *February 28, Computerworld* – (International) **Infected Android app runs up big texting bills.** A rogue Android application tweaked by hackers can hijack a smartphone and run up big texting bills before the owner knows it, Symantec said February 28. The newest in a line of compromised Android apps, said a principle security response manager at Symantec, is Steamy Window, a free program that Chinese hackers modified, then re-released into the wild. The cyber criminals grabbed a copy of Steamy Windows, then added a backdoor trojan horse — "Android(dot)Pjapps" by Symantec's label — to the app's code. The reworked app is placed on unsanctioned third-party "app stores" where unsuspecting or careless Android smartphones find it, download it,

and install it. The trojan planted by the malware-infected Steamy Windows can install other applications, monkey with the phone's browser bookmarks, surreptitiously navigate to Web sites, and silently send text messages, said the Symantec response manager. The last is how the criminals make money. "The Trojan lets them send SMS [short message service] messages to premium rate numbers," he said, for which the hackers are paid commissions.
Source:
http://www.computerworld.com/s/article/9211879/Infected_Android_app_runs_up_big_texting_bills?taxonomyId=17

43. *February 28, Softpedia* – (International) **Russian underground cybercriminal forum hacked.** A closed underground forum that served as a hangout for some of the most notorious Russian cybercriminals was hacked and its entire database was leaked. According to LifeNews(dot)ru, MAZA(dot)la was compromised February 18 by hackers from a rival forum called Direct Connection. Direct Connection is home to the CyberLords Team, the hacking crew of one of the fraudsters who stole $10 million from RBS WorldPay. MAZA(dot)la also had its notorious members, such as "BadB," founder of the CarderPlanet underground marketplace. Russian spammer and malware writer "Severa," was also a MAZA(dot)la forum regular, as well as well known identity thieves "zo0mer" and "My0," who are still wanted by U.S. authorities. In total, MAZA(dot)la had over 2,000 members whose information and private communications are now in the hands of law enforcement authorities. The site was taken offline shortly after the hack and currently remains down.
Source: http://news.softpedia.com/news/Russian-Underground-Cybercriminal-Forum-Hacked-186694.shtml

For another story, see item **13**

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. *February 28, Miami Herald* – (International; North Carolina) **Feds investigate Haitian campaign robo-calls in the U.S.** The U.S. Federal Communications Commission is investigating a series of fervent campaign "robo-calls" in 2010 by a Haitian presidential candidate, which led to evacuations at the Fort Bragg military base in North Carolina, the Miami Herald has learned. In the weeks prior to Haiti's November election, anyone who had ever placed a call to Haiti received a string of pre-recorded calls from the presidential candidate. After the January 12 earthquake, the list included countless Haitian Americans, journalists, non-profit groups, and the U.S. military. On November

17, the Army criminal investigations team swept the cleared buildings for explosives and listened to recordings left on voice mailboxes, a spokesman said. But the U.S. Telephone Consumer Protection Act has specific rules for automated pre-recorded calls: They cannot go to cellular phones when the receiver has to pay for the call. On residential lines, there needs to be full disclosure on whom the call is coming from and how to reach that person. The law applies not only to calls made within the United States, but also to calls made from outside the country to U.S. phones.
Source: http://www.miamiherald.com/2011/02/28/2090704/the-fcc-is-investigating-haiti.html

45. *February 28, Albany Times-Union* – (New York) **Glitch interrupts Oscars on WTEN.** Some television viewers in Albany, New York, had a frustrating time tuning into the Oscars February 27 when a Time Warner Cable equipment failure interrupted reception for almost an hour. Service to News 10 (WTEN) abruptly cut out about a quarter to 8 p.m., just before the Academy Awards began, the station's news director said. The station quickly posted online alerts that directed viewers to Channel 554 and to streaming video on its Web site. A piece of equipment had failed in the Albany area, a spokeswoman for Time Warner Cable in the Northeast said. She did not know specific details about the situation."Engineers quickly jumped on the issue, identified the piece of equipment that failed, turned around, and made sure service was restored," the news director said. She estimated that service was down for less than an hour.
Source: http://www.timesunion.com/local/article/Technical-glitch-interrupts-first-part-of-Oscars-1033620.php

46. *February 28, Reno Gazette-Journal* – (Nevada) **Fire knocks out KNPB service outside of Reno area.** A weather-related fire February 27 that destroyed a KNPB broadcasting transmitting filter caused viewers of the television station outside the Reno, Nevada, area to lose the station's signal on their televisions for several more days. The programming vice president said February 28 the filter system destroyed on Red Peak eliminated the broadcast of KNPB channels for viewers who do not subscribe to Charter Cable channels and those who have certain satellite systems. The programming president said the signal was knocked out at 8:38 p.m. February 27 during the premiere of the station's new production of "Stewards of the Rangeland." A snow and ice storm caused a chemical fire that did not require the response of the fire department. The station has ordered a replacement for the filter, which could take a week or more to obtain. During that time, the signal will still be lost to certain viewers.
Source: http://www.rgj.com/article/20110228/NEWS/110228023/1321

For another story, see item **42**

[Return to top]

Commercial Facilities Sector

47. *March 1, Sun-Times Media Wire* – (Illinois) **Suspect held after apartment firework-sparked blaze injures baby, 36 displaced.** Thirty-six people were displaced and a suspect was in police custody after he lit a firework during a domestic disturbance

February 28 in an apartment in the Austin neighborhood of Chicago, Illinois, sparking a fire that burned a 6-month-old girl. The male suspect was in police custody but was not yet charged as of March 1, police said. The fire started about 9 p.m. on the second floor of a 4-story apartment building at 723 N. Central Avenue, a fire media affairs spokesman said. The blaze was elevated to a still-and-box alarm, and an EMS Plan 1, which automatically sends five ambulances to the scene, was called as a precaution because of the number of people in the building. The fire apparently started when the suspect lit a firework in the apartment during a domestic disturbance. The 6-month-old girl was taken to Children's Memorial Hospital in "stable to critical condition," he said. Paramedics also took one person in good condition to West Suburban Medical Center in Oak Park. Another person was treated on the scene and released.
Source: http://www.myfoxchicago.com/dpp/news/metro/firework-fire-apartment-baby-injured-displaced-central-20110301

For more stories, see items **17** and **24**

[Return to top]

National Monuments and Icons Sector

48. *March 1, Associated Press* – (Texas) **About 120,000 acres burn in Texas wildfires.** About 120,000 acres have burned in West Texas as the wind eased and crews brought all of the fires under control. A spokesperson with the Texas Forest Service (TFS) said March 1 that firefighters were putting out hot spots at various locations. He said the high fire danger would continue throughout the week, but it was much improved since wildfires broke out February 27. Lighter winds February 28 helped with firefighting efforts. TFS responded to fires that blackened about 120,000 acres, but the number could go higher when volunteers file their reports on other blazes they fought. Aircraft assigned to firefighting duty were able to fly February 28, a day after being grounded during strong winds.
Source: http://www.chron.com/disp/story.mpl/ap/tx/7450946.html

[Return to top]

Dams Sector

49. *March 1, Dayton Daily News* – (Ohio) **Flood warnings still in effect.** The flood warnings issued February 28 for sections of the Great Miami River in Ohio were still in effect early March 1. The warnings were for the areas of the river at Taylorsville, Troy, and Sidney. These warnings were likely to continue into March 2. The river was at nearly 20 feet at 2 a.m. Flood stage is 22 feet, according to the National Weather Service (NWS) in Wilmington. Forecasters expected the river to rise to near 22.3 feet by the evening of March 1 and then fall below flood stage after midnight. The high water has caused some roads to be shut down or have the potential for hazardous driving conditions. Communities protected by flood walls and levees can remain protected at a flood stage of 60 feet. NWS February 28 said flooding was a threat in all 88 of Ohio's counties. Wind gusts of 60 mph or more caused roof damage, uprooted

trees and downed power lines. About 3,000 Dayton Power & Light customers lost service early February 28, and all but a handful had their service restored by 6 p.m.
Source: http://www.daytondailynews.com/news/dayton-news/flood-warnings-still-in-effect-1093960.html

50. *March 1, Midland Daily News* – (Michigan) **Deal will allow Sanford Dam work to be completed, lake levels to rise.** An agreement between the Sanford Lake Preservation Association and Boyce Hydro LLC has given new optimism to residents who live along Sanford Lake in Sanford, Michigan that the lake, along with temperatures, will rise again this spring. The two groups announced February 28 that the preservation association "has agreed to provide the funding necessary to implement construction of the Phase Two Sanford Dam embankment repairs mandated by the Federal Energy Regulatory Commission." In anticipation of the agreement and with a sunny sky overhead, repair work began on the dam, which has been drawn down since mid-August of last summer.
Source: http://www.ourmidland.com/story_prep/article_360395ac-ba0c-581d-8719-3c9c85398537.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact Information

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

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer