Homeland Security

Daily Open Source Infrastructure Report for 15 June 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The Associated Press reports that Cargill Inc.'s Wilbur Chocolate plant in Lancaster County, Pennsylvania is shut down while federal officials look into a possible case of product tampering. (See item **24**)
- According to Sky News, Italian police have thwarted a suspected plot to attack next month's G8 summit in Italy which world leaders including the U.S. President and the U.K. prime minister are due to attend. Six people were arrested and accused of criminal association for the purposes of terrorism and arms possession. (See item **32**)

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. *June 12, Foster's Daily Democrat* – (New Hampshire) **Oil tanker moored after striking bottom in the Piscataqua River.** With a damaged rudder, a 528-foot Denmark-based oil and chemical tanker is moored at the Irving Pier after striking bottom in the Piscataqua River near the corporation's terminal late night on June 10,

Coast Guard officials say. Coast Guard officials say there are no signs of pollution to the surrounding waterway due to the accident involving the Torm Mary. The tanker struck bottom around 10:30 p.m. Coast Guard station Portsmouth Harbor dispatched a 25-foot response boat crew at 11:19 p.m. after receiving a report that Torm Mary's stern had struck the bottom of the riverbed. Marine Safety Detachment Portsmouth Harbor sent a marine casualty investigator and inspector and a pollution investigator to the tanker to determine the extent of the damage. Following the incident, the crew onboard the tanker was instructed to stay in port until a dive survey and an inspection was completed by a risk management company. An independent investigator is expected on the scene June 12. Drug and alcohol tests were conducted on the involved parties, all of which produced negative results. "We will work with the tanker's crew to ensure the vessel is structurally sound before it leaves port," said a lieutenant in charge of the Marine Safety Detachment Portsmouth Harbor. Port director said it is a "rare" occurrence when something like that happens. And while it is a concern, he said he continues to have a lot of confidence in the pilots who guide the tankers upstream into their docked positions, he said. "The pilots are licensed by us," he said. "But right now it's a federal matter and I will wait until the Coast Guard is finished with their investigation and I will see the reports and talk to investigating officers."
Source:
http://www.fosters.com/apps/pbcs.dll/article?AID=/20090612/GJNEWS_01/706129901/-1/FOSNEWS

2. *June 12, Hagerstown Herald-Mail* – (West Virginia) **Portion of southbound I-81 reopened after crash.** A portion of southbound Interstate 81 in northern Berkeley County, West Virginia reopened just after 10 a.m. on June 12 following a fiery crash at exit 23 near Marlowe, West Virginia, authorities said. Southbound I-81 is open to exit 23, Maryland State Police said. Traffic will be rerouted onto U.S. 11, then diverted around the crash scene, re-entering I-81 from Hammonds Mill Road at Exit 20. A sergeant of the West Virginia State Police said it is hoped that the highway would be completely open by noon. The accident involving a passenger vehicle and a tanker truck carrying 8,500 gallons of gasoline took place at about 2 a.m., according to the Berkeley County Homeland Security director. The truck driver was uninjured. The driver of the passenger car, a rented Chevrolet Aveo, was still unaccounted for at 10:30 a.m., authorities said. The tanker was delivering fuel from Mechanicsburg, Pennsylvania to the ROCS convenience store off exit 13 of I-81 in Martinsburg. The vehicles collided at the bridge near exit 23. Both burst into flame. The Aveo remained on the bridge, while the truck continued southbound before pulling off the highway. The tanker fire had been extinguished by 10 a.m. and the remains of the vehicle were about to be towed from the scene. The tanker had melted as a result of the fire. Northbound I-81 reopened at about 8:45 a.m. The Homeland Security director said that because the fuel contained ethanol, crews did not have the foam needed to control the blaze.
Source: http://www.herald-mail.com/?cmd=displaystory&story_id=224886&format=html

3. *June 12, Bloomberg* – (Louisiana) **Valero units remain down indefinitely at St. Charles refinery.** Valero Energy Corp. has not determined when it will restart units at

the St. Charles refinery in Norco, Louisiana. “The vacuum, crude and coker units all remain down,” said a company spokesman. “We haven’t established a timetable yet for possible restart.” The units were shut June 9 after a minor fire. The 185,000-barrel-a-day refinery processes primarily Maya and Mars crude oil, and distributes products to the East Coast and Midwest by pipeline and barge.
Source: http://www.bloomberg.com/apps/news?pid=20601072&sid=aIj6o61fZ.wM

[Return to top]

Chemical Industry Sector

4. *June 11, Janesville Gazette* – (Wisconsin) **Crews respond to anhydrous ammonia spill.** The Rock County Sheriff’s Office, Wisconsin State Patrol, Rock County Public Works, the Janesville Fire Department, and the Town of Turtle Fire Department are tending to what is being called a minor spill of anhydrous ammonia in the area of Avalon Road just east of County Highway J, southeast of Janesville. Crews were called out at 10:01 a.m. on June 11 to a report of a spill resulting from an overturned vehicle. At about noon, firefighters were preparing to offload the remaining ammonia from the damaged tank to a new tank brought in for that purpose. The damaged tank was on a trailer, being towed by a large tractor eastward on Avalon Road. The trailer appeared to have turned onto its side, damaging the tank and leaking the white smoky gas. No residences were in the immediate area, and no one appeared to have been hurt. Approaches to the scene on County J and Avalon Road/Highway 11 continue to be blocked by Rock County Sheriff’s deputies and the State Patrol. Traffic is not being allowed through.
Source: http://gazettextra.com/weblogs/latest-news/2009/jun/11/crews-respond-anhydrous-ammonia-spill/

5. *June 11, Daily Dunklin Democrat* – (Missouri) **Chemical spill cues mayor to request designated truck route.** Following the incident on June 8, involving a tanker truck turnover that resulted in a chemical spill of 3,500 gallons of liquid fertilizer, city officials have been queued to request a designated truck route around Kennett’s downtown district. According to the mayor, to his knowledge, a formal request for a truck route had not been previously sent in to the Missouri Department of Motor Vehicles (MoDOT). The traffic operations engineer with MoDOT was asked about the possibility of a truck route, to which he responded, “I do not know that we have been formally approached [about a truck route]. We would be open to discuss it with [city officials].” A truck route could definitely be a possibility. However, since the highway that travels through Kennett is a State highway, State Highway 84, MoDOT legally cannot make the large trucks stop coming through town. Even if the truck route is not established in Kennett, there is still the possibility that the HAZMAT trucks could be rerouted, with advanced warning given to Kennett’s Emergency Management responders.
Source: http://www.dddnews.com/story/1546620.html
See also: http://www.columbiamissourian.com/stories/2009/06/09/kennett-spill-wasnt-hazardous-it-was-smelly/

6. *June 11, WAVE 3 Louisville* – (Kentucky) **Employee burned in explosion at resin plant.** One person is in the hospital with severe burns after an explosion on June 11 at a Louisville plant. The blast happened just after noon at the Nuplex Resins plant. That explosion made for some frightening moments at the Crittenden Drive plant. A veteran employee was cleaning what is known as a pilot reactor vessel, basically a big 180-gallon kettle, when the blast occurred. It was a routine job and the employee was using a common solvent, one that happens to be in Windex. "It is a pressure vessel and for reasons we have not been able to determine we had a leak from the vessel itself that allowed vapors to accumulate in the building that it is contained in," said the health and safety manager at Nuplex Resins. Plant and fire officials say they are still trying to determine what ignited the vapors. The explosion was so strong that it blew off two steel doors. The room's ceiling gave way above the kettles just as it is designed to do in an explosion.
   Source: http://www.wave3.com/Global/story.asp?S=10517182

7. *June 11, Chattanooga Times Free Press* – (Georgia) **Fire, safety violations shut down Ga. chemical plant.** Dalton fire officials discovered a number of safety violations at the Vericol plant site and temporarily have closed down the facility. Vericol was a chemical and adhesive manufacturing plant. The Dalton fire department captain, city fire marshal and safety coordinator said Vericol operated in Dalton for several years but since has closed. Chemence Inc. has operated a nail product production company at a building on the site for about a year. The safety violations include improper storage of hundreds of chemical containers up to 200 gallons in size and electrical, emergency lighting and emergency exit issues, as well as an inoperable sprinkler system. Samples revealed chemicals were leaking onto building floors. In response to all of the safety concerns the buildings were condemned and utilities for the buildings were ordered to be turned off on June 10. Steps taken so far the week of June 8 will be the first in an ongoing and lengthy investigation to include representatives from Georgia's Occupational Safety and Health Administration and the Georgia Environmental Protection Division.
   Source: http://www.firerescue1.com/firefighter-safety/articles/502242-Fire-safety-violations-shut-down-Ga-chemical-plant/

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

8. *June 12, WWAY 3 Wilmington* – (North Carolina) **Brunswick nuclear plant under investigation.** The Nuclear Regulatory Commission is investigating Brunswick Nuclear Plant in Southport. Progress Energy, which oversees the plant, confirmed the investigation is looking into the professional conduct of some of the plant's security officers. The company would not go into detail, but assured the plant is secure. It added the investigation should wrap up in the next few days.
   Source: http://www.wwaytv3.com/node/16357

[Return to top]

Critical Manufacturing Sector

9. *June 12, Reliable Plant* – (International) **Counterfeit SKF bearings seized in Czech Republic.** During April 2009, the SKF Group, working in cooperation with the Czech police authorities, made a raid and confiscated more than 30 tons of counterfeit SKF bearings at a non-authorized dealer in the North-East region of the Czech Republic. In addition, products from other bearing manufacturers were confiscated. This dealer has been purchasing these products from non-SKF sources and selling them to both end-users and other dealers in the Czech Republic as well as other countries, mainly in Europe. The manufacture and trade of counterfeit products is a growing global problem which increasingly affects all brands and all markets. Counterfeit SKF products and other bearing brands being manufactured and sold in the marketplace is not only illegal but also puts the end customer at a major risk since they purchase and use these products thinking that they have received genuine products. The use of counterfeit SKF products in an application can in worst case put the user, employees and the public in a serious safety risk or result in shorter service life, poor product quality or damage to equipment. SKF is a leading global supplier in the areas of bearings, seals, mechatronics, services and lubrication systems.
   Source:
   http://www.reliableplant.com/article.aspx?articleid=18151&pagetitle=Counterfeit+SKF+bearings+seized+in+Czech+Republic

10. *June 12, Reliable Plant* – (New Hampshire) **OSHA seeks $255K fine vs. Sturm Ruger & Company.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has proposed $255,150 in fines against Sturm Ruger & Company Inc. for 60 alleged violations of safety and health standards identified during the agency's inspections of the firearms manufacturer's Newport, New Hampshire plant conducted between November 2008 and May 2009. "Our inspections identified a large number of mechanical, respirator protection, electrical, lead, fire, explosive and other hazards that must be effectively and continuously addressed to protect the workers at this plant from potentially deadly or disabling injuries and illnesses now and in the future," said the OSHA's area director in New Hampshire. OSHA found that the company failed to guard rotating parts on drill presses, sanding and polishing machines despite its knowledge that employees were exposed to severe or fatal injuries if they came in contact with the rotating parts. As a result, OSHA has issued the company one willful citation with $63,000 in proposed fines. OSHA defines a willful violation as one committed with plain indifference to or intentional disregard for employee safety and health.
    Source:
    http://www.reliableplant.com/article.aspx?articleid=18180&pagetitle=OSHA+seeks+%24255K+fine+vs.+Sturm+Ruger+%26+Company

[Return to top]

Defense Industrial Base Sector

11. *June 11, WMUR 9 New Hampshire* – (National) **Shea-Porter files bill to punish negligent defense contractors.** A U.S. Representative has introduced legislation to punish defense contractors if they have previously been found guilty of causing serious injury or death of government personnel. The bill would prevent those defense contractors from receiving additional government contracts for five years. The bill was prompted by incidents in which at least three service members were electrocuted while showering at U.S. facilities in Iraq. Others have been injured or killed in other electrical incidents, according to an Associated Press report. The Safety in Defense Contracting Act has been endorsed by the Iraq and Afghanistan Veterans of America, the Military Officers' Association of America, the National Guard Association of the United States and the Veterans of Foreign Wars.
    Source: http://www.wmur.com/politics/19724914/detail.html

For more stories, see items **9** and **10**

[Return to top]

Banking and Finance Sector

12. *June 12, Courthouse News Service* – (International) **SEC alleges cold-blooded bank scam.** Four people and their three companies defrauded investors of millions of dollars in a prime-bank scam, claiming their investment plan had to be kept secret because if people knew about it, it would encourage "the flight of capital from the United States," the SEC claims in Federal Court. The SEC sued the four defendants, Morgan European Holdings ApS aka Money Talks, ApS, and Bowman Marketing Group. According to the SEC complaint, the defendants raised $14 million or more by promising monthly returns of 14 to 70 percent. The defendants sent $4.5 million to Denmark, and then sent it back to themselves in the United States. The SEC says the defendants' pitches "describe the operation of a class prime bank scheme." They used apparently sophisticated, conspiratorial language to gull 150 or more victims. For example, some of these materials describe how the 'top fifty financial institutions' or the U.S. Federal Reserve trade with each other to 'artificially inflate the money supply' for international commerce. According to the offering materials distributed by one of the defendants, participants were to provide money to supply 'the margin' for a trader to pass a 'debenture or treasury' to the end user, generating returns through the leveraging of financial instruments. "The materials distributed by one of the defendants stated that these programs were secret but real, even though the 'official position' of the U.S. government was that such trading programs did not exist so as 'to increase the participation in traditional investments and reduce the flight of capital from the United States." After the fraud was discovered, the defendants "urged investors not to cooperate with the Commission or other authorities."
    Source: http://www.courthousenews.com/2009/06/12/SEC_Alleges_Cold-Blooded_Bank_Scam.htm

13. *June 12, Bloomberg* – (International) **Italian police ask SEC to authenticate seized U.S. Treasuries.** Italy's financial police said they asked the U.S. Securities and Exchange Commission to authenticate U.S. government bonds found in the false bottom

of a suitcase carried by two Japanese travelers attempting to cross into Switzerland. The bonds, with a face value of more than $134 billion, are probably forgeries, a colonel of the Guardia di Finanza in Como, Italy, said on June 12. If the notes are genuine, the pair would be the U.S. government's fourth-biggest creditor, ahead of the U.K. with $128 billion of U.S. debt and just behind Russia, which is owed $138 billion. The seized notes include 249 securities with a face value of $500 million each and 10 additional bonds with a value of more than $1 billion, the police force said on its Web site. Such high denominations would not have existed in 1934, the purported issue date of the notes, the colonel said. Moreover, the "Kennedy" classification of the bonds does not appear to exist, he said. The bonds were seized in Chiasso, Italy. The colonel said he expects a determination from the SEC "within a few days."
Source: http://www.bloomberg.com/apps/news?pid=20601092&sid=afJXAA1ahZyo

14. *June 11, St. Louis Business Journal* – (Missouri) **Father-and-son developers indicted in multimillion fraud scheme.** A father and son have been indicted on multiple charges involving a broad-ranging bank fraud and money laundering scheme that covered nearly three years affected five local banks and involved commercial loans of nearly $5 million. The defendants, of Creve Coeur, have been indicted by a federal grand jury on five felony counts of bank fraud, three felony counts of money laundering and a forfeiture count involving personal and real property financed by the alleged scheme, the U.S. attorney's office for Eastern Missouri said. The defendants were in the real estate development business under the name Real Estate Management Services LLC and sought to develop five residences in Ladue and other high-end suburbs. In order to obtain financing for these developments, the defendants are alleged to have submitted phony income tax returns, sales contracts and financial statements, according to the indictment. The government seeks two of the residential properties that remain in the name of the defendants' business, a vehicle and a diamond ring purchased with proceeds from the fraud.
Source: http://www.bizjournals.com/stlouis/stories/2009/06/08/daily57.html

15. *June 11, Reuters* – (New Jersey) **NJ mortgage exec pleads guilty in $140 million fraud.** The former president of U.S. Mortgage Corp, a New Jersey mortgage lender and broker that filed for bankruptcy in February, has pleaded guilty to two criminal conspiracy charges in a $139.6 million scheme to defraud credit unions and others, prosecutors said. The defendant pleaded guilty in federal court in Newark, New Jersey, to one count of mail and wire fraud conspiracy and one count of money laundering conspiracy, according to the acting U.S. Attorney for the District of New Jersey. The defendant is expected to be sentenced under a plea deal to between 12-1/2 and 20 years, and to pay restitution to victims. A U.S. District Judge scheduled an October 1 sentencing hearing. She allowed the defendant's release on a $1 million bond to home confinement. The defendant admitted to conspiring with others from January 2004 to January 2009 to fraudulently sell credit union loans, and use proceeds to finance U.S. Mortgage's operations and investments for himself and the Pine Brook, New Jersey-based company, prosecutors said. He also admitted to diverting funds that should have been paid to credit unions for mortgage loans that were to be sold to Fannie Mae, to help offset bad investments that he had made in mortgage-backed securities, prosecutors said.

Source: http://www.reuters.com/article/domesticNews/idUSTRE55A72J20090611

16. *June 11, Reuters* – (International) **S.Africa fraud worth up to $1.2 billion uncovered.** Hundreds of investors have been fleeced of up to 10 billion rand ($1.2 billion) in what could be South Africa's biggest corporate fraud, a private investigator and lawyer representing investors said. A South African businessman living in Australia, was said to have lured investors with the promise of 200 percent annual returns linked to pharmaceutical imports, and forged AIDS drug orders to reassure its funders when money started to dry up. The scheme is still unraveling, but lawyers and investigators believe hundreds of investors, including top businessmen from South Africa, the United States, Germany and Australia, were involved. The case looks set to rank as South Africa's biggest corporate fraud and has shocked the country's business community, known for its conservative approach to risk and investment.
Source: http://www.reuters.com/article/marketsNews/idUSLBO2543820090611

17. *June 11, MSNBC* – (National) **Most banks still getting weaker, analysis shows.** Bad loans on real estate continue to push harder on the nation's banks. At the end of the first quarter, six out of every 10 banks in the U.S. were less well prepared to withstand their potential loan losses than they had been at the end of 2008, according to a new analysis by msnbc.com and the Investigative Reporting Workshop at American University in Washington. Overall, bad loans rose another 22 percent in the quarter as the recession continued. Msnbc.com is publishing information on the nation's 400 largest banks as well as all banks with high ratios of troubled loans to assets. Information on the financial health of more than 8,000 banks nationwide is available at the updated BankTracker site published by the American University group. The analysis relies on information reported through March 31 to the Federal Deposit Insurance Corp., calculating each bank's troubled asset ratio, which compares troubled loans against the bank's capital and loan loss reserves. A similar ratio, known as a Texas Ratio, is commonly used by bank analysts as a snapshot of a bank's financial health, though it cannot capture all the nuances of a bank's condition. Although much attention has been focused on surprising profits at U.S. banks in the first quarter of 2009, under the surface lurks an industry still suffering from the recession. If an individual sets aside the 10 largest banks, the rest of the industry lost money in the quarter, primarily because of very large losses at a few banks. While the 10 largest banks reported $10.2 billion in earnings for the quarter, the remaining 8,245 banks together lost $2.6 billion, according to the analysis. One in five banks lost money in the quarter, and several lost big, weighing down the rest. Four large banks account for more than $5 billion in losses. Huntington National Bank of Columbus, Ohio, lost $2.46 billion. FIA Card Services of Wilmington, Del., lost $1.47 billion. SunTrust Bank of Atlanta lost $783 million. Sovereign Bank of Wyomissing, Pa., lost $764 million.
Source: http://www.msnbc.msn.com/id/31193659/

18. *June 10, Washington Post* – (National) **Spear-phishing gang resurfaces, nets big catch.** A prolific phishing gang known for using sophisticated and targeted e-mail attacks to siphon cash from small to mid-sized business bank accounts appears to be back in operation after more than a 5-month hiatus, security experts warn. From

February 2007 to January 2009, analysts at Sterling, Virginia-based security intelligence firm iDefense tracked 38 separate phishing campaigns from am Eastern European gang they simply call "Group A." iDefense believes this group was one of two responsible for a series of successful phishing attacks that spoofed the U.S. Better Business Bureau (BBB), the U.S. Department of Justice, the IRS, as well as Suntrust and payroll giant ADP. Last summer, authorities in Europe and Romania are thought to have arrested most members of a rival BBB phishing gang that iDefense called Group B. While the type of tricks that Group A employs once victims are hooked have grown more sophisticated, the initial lure used to snare people has not changed: In each attack, the scammers send out "spear phishing" e-mail messages (so called because they use the victim's name in the message) and urge the recipient to click on an attachment. The attached file is, naturally, a Trojan horse that steals stored user names and passwords, and looks for victims logging in at commercial banks. If the victim logs in to a bank that requires so-called two-factor authentication — such as the input of a one-time pass phrase or random number from a supplied hardware token — the Trojan re-writes the bank's Web page on the fly, inserting a form that requests the information. The attackers typically begin initiating wire transfers out of the victim accounts shortly after the credentials are stolen, said an iDefense analyst.
Source: http://voices.washingtonpost.com/securityfix/2009/06/spear-phishing_gang_resurfaces.html?wprss=securityfix

[Return to top]

Transportation Sector

19. *June 12, Parkersburg News and Sentinel* – (West Virginia) **Flights resume at airport.** Flights resumed June 11 at the Mid-Ohio Valley Regional Airport where repairs are still being made to power lines damaged by a storm on June 8, the airport manager said. Colgan Air canceled flights on June 9 and June 10 after power was cut to a separate building that houses the communications equipment that sends weather data to commercial airplanes. The airport is being powered by generators and a temporary line was run June 10 to the building to power the weather communications equipment used by the National Weather Service and the Federal Aviation Administration air traffic control tower. A severe storm blew through the region around 4 p.m. June 8. Lightning strikes damaged the circuits and lines and blew breakers at the airport where crews have been working to repair. Repairs made June 10, which included splicing a cable that was burned away during the storm, did not work, indicating other parts of the underground lines might have been affected, the airport manager said.
Source: http://www.newsandsentinel.com/page/content.detail/id/518268.html?nav=5061

20. *June 12, Reno Gazette-Journal* – (Texas) **Dallas weather disrupts Reno flights.** A series of powerful thunderstorms in Dallas disrupted June 11 airline traffic at Reno-Tahoe International Airport. "We have at least six flights so far that have been canceled or substantially delayed," an airport spokesman said. "We expect more through the day." The Associated Press reported the storms grounded or delayed almost 100 flights at two Dallas-area airports. The weather also left about 150,000 north Texans without power. The spokesman said Dallas-Fort Worth International Airport, the third busiest airport in

America, is a major hub for American Airlines and Southwest Airlines. "What we're seeing here is truly a ripple effect from there," he said. "Flights are not getting in or getting out from Dallas, so that is truly impacting the system."
Source: http://www.rgj.com/article/20090612/NEWS/906120422/1321

21. *June 11, Atlanta Journal-Constitution* – (Georgia) **Flights delayed after emergency landing at Hartsfield-Jackson.** One runway remains closed at Hartsfield-Jackson Atlanta International Airport following the emergency landing of a commuter jet, airport officials said. The Federal Aviation Administration is reporting departure delays of up to 45 minutes because of the small Atlantic Southeast Airlines regional jet. An ASA spokeswoman said the plane had trouble engaging its landing gear just before 7 p.m. Delta Flight 5414 reported the need to make an emergency landing around 6:42 p.m. on June 11, another airport spokesman said. Hartsfield emergency vehicles were on the scene when the plane landed in the event of a crash, but were not needed, he said. The single runway — one of five — is closed while the National Transportation Safety Board investigates the cause of the malfunction, officials said. The 19 passengers and three crewmembers on board the flight from Columbus, Georgia, to Atlanta, Georgia were uninjured.
Source:
http://www.ajc.com/gwinnett/content/metro/stories/2009/06/11/emergency_landing.html

22. *June 11, WSBT 2 South Bend* – (Michigan) **Bridge closure could last for three years.** Years of water damage forced officials in Cass County, Michigan, to close a heavily traveled road. Redfield Street was closed between Adamsville and Cassopolis roads recently because the bridge, located 0.5 miles north of Indiana running east–west over Christiana Creek, is not safe for the 2,500 cars that pass over it every day. Michigan's budget problems could make this a long time problem for drivers. The wooden structure bridge has too many problems to be fixed and needs to be replaced. But with a $1 million price tag, it could take three years or longer to receive the funds from the Michigan budget. "We're investigating ways we could fix the bridge to the extent that we make it safe and allow some commercial traffic to go over it. Will we ever have trucks go over that bridge until it gets replaced? No," said a Cass County road commission spokesman. While the bridge closure is an inconvenience, people in the area say they are more concerned about a potential increase in emergency response time.
Source: http://www.wsbt.com/news/local/47881067.html

23. *June 10, Federal Computer Week* – (Virginia) **IG: Dulles IT security needs more work.** The Department of Homeland Security (DHS) needs to update its computer servers and upgrade physical protection for information technology systems at Dulles International Airport in Virginia, according to a new report from the DHS Inspector General. DHS' Transportation Security Administration, along with U.S. Customs and Border Protection (CBP), which both operate systems at Dulles, have undertaken corrective measures since the IG reported in January 2007 that critical IT systems there were at risk of being exploited and their missions disrupted. However, both agencies need to do more work on physical security controls, including using locked cabinets, and on updating technical controls, including installing updated servers with the latest

release of operating system software, according to the report posted on the Web June 9. "The department has made significant progress in improving technical security for information technology assets at Dulles. Further work is needed to comply with government policies and procedures," the report states. CBP officials agreed with the recommendations, and Transportation Security Administration officials agreed with most of the recommendations, according to comments included in the report.
Source: http://fcw.com/Articles/2009/06/10/Dulles-IT-security-needs-work-IG-says.aspx

For more stories, see items **2**, **4**, and **5**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

24. *June 12, Associated Press* – (Pennsylvania) **Feds investigate 'foreign material' at chocolate plant.** Production at a Lancaster County, Pennsylvania chocolate plant is shut down while federal officials look into a possible case of product tampering. A representative for Cargill Inc. says three pieces of "foreign material" were discovered at the Wilbur Chocolate plant in Lititz, and the FBI and the Food and Drug Administration are investigating. The plant may not reopen for several weeks. Only one-third of the employees will report to work and they will be cleaning the plant. The representative would not say what kind of foreign material was found. The workers' union has been trying to reach a contract agreement for more than two years. A representative says only that the two sides are negotiating in good faith.
Source: http://www.philly.com/inquirer/breaking/business_breaking/20090612_Feds_investigate_foreign_material_at_chocolate_plant.html

25. *June 11, USAgNet* – (International) **Russia expands ban on U.S. imports of pork, chicken.** Russian regulators are expanding bans on pork and other meat imports to more U.S. states, citing swine flu fears. According to the Associated Press (AP), the decision to include Wisconsin, Washington and Illinois brings the number of states affected by the ban on pork, chicken and other meat imports to seven. Pork imports are already banned from four other states. A spokesman for the agricultural oversight agency Rosselkhoznadzor says the move is temporary and meant to protect Russians from the disease. The spokesman said on June 9 that the agency still has questions about what steps the United States is taking to prevent the disease's spread, the AP reports. U.S. officials complain that humans can not get swine flu from eating pork and that the ban is designed to protect Russian producers.
Source: http://usagnet.com/story-national.php?Id=1261&yr=2009

[Return to top]

Water Sector

26. *June 12, Associated Press* – (California) **S.F. Bay treatment plant operator facing fines for spills.** A sanitation district that operates a treatment plant on San Francisco Bay is facing fines of up to $332,000 for spills that sent wastewater into the bay. State water regulators say in three separate incidents, the Sausalito-Marin City Sanitary District's treatment plant at Fort Baker sent a combined 775,000 gallons of partially treated or raw sewage into the bay. Officials with the San Francisco Regional Water Quality Control Board say in the biggest spill, nearly 767,000 gallons of partially treated wastewater flowed into the bay between February 15 and 21 when an underwater pipe burst. The district is also being blamed for a smaller discharge of raw sewage in August of 2008. A hearing is set for September 9.
Source:
http://www.recordnet.com/apps/pbcs.dll/article?AID=/20090612/A_NEWS/90612001/-1/NEWSMAP

27. *June 11, Orlando Sentinel* – (Florida) **Polk County fined $12,000 for CWA violations.** The Polk County Board of Commissioners was fined $12,150 for not properly disposing sewage sludge at its wastewater treatment plant in Bartow, the U.S. Environmental Protection Agency (EPA) announced June 11. EPA officials found the plant's sewer sludge contained excessive levels of molybdenum, an element that can be found in agricultural soils, from 2002 to 2004, violating the Clean Water Act (CWA). The county also was cited for failing to monitor sewage sludge during the second quarter of 2006. The EPA penalized nine others throughout the southeast part of the country, including the Port of Pensacola and the Aqua Utilities Inc. in Florida, for violating the CWA.
Source: http://www.orlandosentinel.com/news/local/southwest/orl-bk-polk-county-fined-for-cwa-violations-061109,0,4764374.story

28. *June 9, Columbus Ledger-Enquirer* – (Georgia) **Water Works refuses to release report on tank collapse.** The Columbus Water Works Board of Commissioners and utility officials refused on June 8 to release to the public details on the cause of the April water tank collapse. Local engineering firm Jordan Jones and Goulding hired Krebs and Associates of Birmingham to examine the 32-foot high steel tank to see what caused it to fail and spill 6 million gallons of Chattahoochee River water near the intersection of J.R. Allen Parkway and River Road. The tank collapse on April 25 caused property damage to areas surrounding the North Columbus Water Works plant. The Water Works president was asked to release a copy of the report at the conclusion of the scheduled board meeting. "I am not going to release the report at this time on advice of my attorney," he said. Commission members met with attorneys of Hatcher Stubbs Land Hollis and Rothschild LLC. The meeting was closed to the public. One of the attorneys cited a provision in the Georgia Open Records Act that allowed the closed session to discuss potential settlements. The board approved an emergency contract to replace the water tank during their meeting on June 8. Instead of one 6-million gallon steel tank, the Water Works is going to replace it with two 4-million gallon concrete tanks. The tank

was used to hold raw river water awaiting treatment. “We’re operating OK,” the Water Works president said. “But we certainly have diminished capacity to answer any other emergency situation.” Construction on the new tanks by Precon Corp. of Newberry, Florida, is expected to begin August 1. The first tank could be in use by December and the second one sometime early next year.
Source: http://www.ledger-enquirer.com/news/story/743313.html

[Return to top]

Public Health and Healthcare Sector

29. *June 12, Agence France-Presse* – (International) **Swine flu vaccine ready for tests.** The Swiss pharmaceutical giant Novartis said on Friday that it has a swine flu vaccine ready for trial as governments stepped up precautions to counter the new declared influenza pandemic. While millions could catch the flu, governments and health experts around the world have sought to play down fears that the A(H1N1) virus could become a major killer. Swine flu has so far infected almost 30,000 people in 74 countries and claimed 145 lives since it was first detected in Mexico in April, according to World Health Organization (WHO) figures. A Novartis spokesman told AFP it hoped to have a vaccine in production by September or October.
Source: http://www.google.com/hostednews/afp/article/ALeqM5jSDgUjzDWtXLH39myt00ZdKM6Vkg

30. *June 12, Miami Herald* – (Florida) **Miami Children’s Hospital water supply under scrutiny.** A state agency will monitor Miami Children’s Hospital in the wake of a county report blaming a common-yet-deadly bacteria for the deaths of two infants in the hospital’s neonatal intensive care unit. The Florida Agency for Health Care Administration will follow the hospital’s compliance with recommendations by the Miami-Dade Health Department to improve its water supply, where 23 strains of the Pseudumonas aeruginosa were found by health investigators. A hospital spokeswoman said Thursday that the hospital will cooperate with the county’s recommendations. The hospital does regular visual checks on the plumbing system and is working to refine the program, she said. The hospital also will monitor chlorine levels and will take advantage of the county’s purge program.
Source: http://www.miamiherald.com/news/southflorida/story/1093339.html

31. *June 9, Frederick News Post* – (Maryland) **Insider threat is biolab’s biggest security issue.** A Defense Science Board report on military biolab safety issued last month identified insider threat as the labs’ biggest security problem. The report’s top recommendation was for a security review of computers that control access to and of the environmental systems’ computers for the labs at the U.S. Army Research Institute of Infectious Diseases, at Fort Detrick in Frederick, Maryland. The environmental systems’ computers help ensure that airborne pathogens cannot leave the labs. Specifically, the report warned that someone could surreptitiously connect those computers to a network, allowing an unauthorized person to access them remotely. The Under Secretary of Defense for Acquisition, Technology and Logistics commissioned the report in October.

Source: http://www.wtop.com/?nid=598&sid=1692364

[Return to top]

Government Facilities Sector

32. *June 11, Sky News* – (International) **G8 attack plot: suspects arrested in raids.** Italian police have thwarted a suspected plot to attack the G8 summit which world leaders including the U.S. President and the U.K. prime minister are due to attend. Six people were arrested and accused of criminal association for the purposes of terrorism and arms possession, an anti-terrorist police chief said. Officers reportedly seized weapons including a bomb during the raids in Rome, Milan, and Genoa. The suspects had maps of the summit's closed-circuit surveillance system and "were trying to figure out how to bypass the security systems," the police chief said. The investigation into the alleged plot started two years ago. According to ANSA.it, the group had plotted to attack the original venue of next month's G8 summit, a former U.S. Navy base on the Sardinian island of La Maddalena, police said. The venue was recently moved to the Abruzzo capital L'Aquila to help it recover from a devastating earthquake in April. The suspected plotters shifted their attention to target the new venue, according to Italian newspapers Corriere della Sera and La Stampa. They were trying to "reconstitute a formation similar to the Red Brigades," a terrorist group who carried out attacks in Italy in the 1970s and 1980s, the police chief said.
    Source: http://news.sky.com/skynews/Home/World-News/G8-Summit-Police-In-Italy-Arrest-Suspects-Over-Plot-On-Meeting-Moved-From-La-Maddalena-To-LAquila/Article/200906215301562?lpos=World_News_Second_World_News_Article_Teaser_Region_0&lid=ARTICLE_15301562_G8_Summit%3A_Police_In_Italy_Arrest_Suspects_Over_Plot_On_Meeting_Moved_From_La_Maddalena_To_LAquila
    See also: http://www.ansa.it/site/notizie/awnplus/english/news/2009-06-11_111383347.html

For another story, see item **11**

[Return to top]

Emergency Services Sector

33. *June 12, KFVS 12 Cape Girardeau* – (Missouri) **Missouri only State that can't track 911 calls from cell phones.** Missouri does not have the technology in place to track certain cell phone numbers or locations when a person calls 911. This is because Missouri is the only State in the country without a cell phone tariff. Emergency management coordinators say that leaves them without the money to buy equipment that would allow 911 operators to track cell phone callers.
    Source: http://www.kfvs12.com/Global/story.asp?S=10519527&nav=menu51_2_3_1

34. *June 11, Government Computer News* – (Minnesota) **Minneapolis/St. Paul, federal DOT test next-generation 911 systems.** The Minneapolis/St. Paul metropolitan region is testing a new regional, IP-based 911 system that would run over a wide area network.

The system would link all of the call centers in the eight-county metro area. Meanwhile, the federal Transportation Department is launching a Next Generation 911 pilot next week at five sites, including one of the sites in the Minneapolis/St. Paul pilot. The Metropolitan Emergency Services Board (MESB) is implementing a two-year pilot project based on the National Emergency Number Association's technical and operational standards. The pilot project will evaluate the network, routing, location data and answering position solutions as well as evaluate how the system could be implemented, managed, maintained and funded. The pilot will be used as a model to implement a regional IP-based 911 system linking all the communication centers together over a wireless are network (WAN). The proposed network design has the capacity to support all of the IP-based public safety applications currently in use, plus any anticipated growth through 2010. These applications include the board's regional GIS location database management system, the Criminal Justice Data Network, the regional 800/700 MHz radio system, a mobile data network, and a secure broadband Internet connection.
Source: http://gcn.com/articles/2009/06/11/minneapolis-dot-test-next-generation-911-systems.aspx

35. *June 11, Florence Times-Daily* – (Alabama) **New training center unveiled.** For two years, members of the Florence, Alabama Police Department have worked with other city departments to turn a 15-acre cotton field into a modern law enforcement training facility. On Thursday morning, with representatives from various state and local agencies and departments on hand, the facility was officially unveiled. The Alabama Attorney said it is imperative to provide tools for law enforcement to be trained so they can be safe and provide protection for the community they serve. The new facility has a 20-lane pistol range with moving, pop-up and running targets; a 12-lane, 100-yard sniper rifle range; and a covered six-room "shoot" house, used for close quarters tactical training. It also has a 3,200-square-foot training building, complete with conference rooms, classrooms and work areas. The facility has an area where the department's bomb squad can practice and train.
Source:
http://www.timesdaily.com/article/20090612/ARTICLES/906125025/1011/NEWS?Title=New-training-center-unveiled

36. *June 11, Washington Post* – (Maryland) **Suspicious package prompts evacuation of Montgomery Crisis Center.** Authorities evacuated the Montgomery County, Maryland Crisis Center in Rockville Thursday night after an agitated patient made threats, then left behind a bag with a box inside the building. The fire department's bomb squad was called at about 8 p.m. for a suspicious package at the center, a department spokesman said. Officials evacuated about two dozen people from the facility. Authorities used a robot to investigate the bag, and found electrical components inside. The bag and box were removed from the building and deemed safe. People were allowed to re-enter the building at about 10:15 p.m.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2009/06/11/AR2009061104628.html

[Return to top]

Information Technology

37. *June 12, The Register* – (International) **Chrome update completes busy browser patch week.** Google has pushed out an update designed to fix a pair of vulnerabilities involving the WebKit application framework that underpins its Chrome browser. The most severe of the two flaws involved a "high risk" memory corruption flaw in WebKit, which creates a potential means for hackers to inject hostile code into the sandbox used by the browser. The second flaw involves a less severe information disclosure risk, involving the Drag and Drop functionality built into WebKit. The update completes a busy week on the browser security front with a significant cumulative update for Internet Explorer on June 9 and a Firefox update on June 11. In addition, Apple released a beta version of its Safari 4 browser. Outside the browser security arena, Adobe released the first of its scheduled patch updates on June 9, and FreeBSD dropped an update designed to defend against a stack-based buffer-overflow that poses a potential code injection risk. It is becoming more difficult for hard-pressed system administrators to keep track of updates, especially when many arrive without any indication a fix is in development. Some security patching experts, such as the director of security operations at nCircle, advocate the creation on a general industry patching day to make the patching process easier to plan and manage.
Source: http://www.theregister.co.uk/2009/06/12/google_chrome_update/

38. *June 11, VNUNet.com* – (International) **Symantec warns of wireless keyboard security threat.** Security firm Symantec has uncovered a new form of attack aimed at users of wireless keyboards. The warning follows the release of Keykeriki, an open-source "sniffer" project that allows users to remotely decode wireless transmissions. Symantec said that this effectively creates a new type of key-logger that could be used by cybercriminals to steal sensitive data such as user names, passwords and bank details. The project was created by a site called remote-exploit.org. "This open-source hardware and software project enables every person to verify the security level of their own keyboard transmissions, and/or demonstrate the sniffing attacks (for educational purpose only)," the site notes. Symantec warned that, although the creator's intentions appear honorable, making the software code and hardware schematics open to everyone means that criminals could use the software to eavesdrop on wireless keyboard inputs. The criminals would not have to install anything on the host system, but would simply have to be in range of the keyboard's wireless signal. Symantec said that future wireless keyboards should introduce encrypted communication between the device and the receiver, and warned those working on office or public computers to resort to wired keyboards for the time being.
Source: http://www.enterprise-security-today.com/story.xhtml?story_id=67095

39. *June 11, InformationWeek* – (International) **Microsoft to launch Morro antivirus 'soon.'** Microsoft on June 11 confirmed plans to kill off its Windows Live OneCare subscription security service in favor of a free offering that will feature a core of essential anti-malware tools while excluding peripheral services, such as PC tune-up programs, found in OneCare. A spokesman for the company told news agency Reuters that Microsoft will launch the free product, code-named Morro, "soon" but did not

provide further details. Microsoft has said previously that Morro will be suitable for use on low-cost, low-powered netbooks that are growing in popularity in emerging markets and in some segments of the North American computer market. Microsoft also is planning to launch versions of Windows 7 that are netbook-compatible. The definition of malware covers a range of computer threats, including viruses, spyware, rootkits, and Trojans. Hackers, many of them connected to organized crime, often use such tools to extract sensitive data like bank account numbers and passwords from users' PCs. Microsoft announced in November that it will launch Morro in this month, at which time it will discontinue the $49.95-per-year OneCare service. As of June 11, Microsoft was still selling OneCare subscriptions. Morro will be compatible with Windows XP, Windows Vista, and the forthcoming Windows 7 operating systems, the company has said. While users and analysts may welcome Microsoft's offer of free antivirus software, competitors such as Symantec and McAfee and government competition watchdogs may not. Microsoft could draw antitrust complaints if it integrates Morro so tightly into Windows that it makes security software from third parties difficult to install or use.
Source:
http://www.informationweek.com/news/security/antivirus/showArticle.jhtml?articleID=217800827

40. *June 11, New York Times* – (International) **More scamming and spamming on Twitter.** Twitter is seeing a surge in activity from the scamming and spamming classes. A spate of phishing attacks have been followed by myriad other efforts to soak Twitter's enthusiastic and rapidly growing user base. Recently, attackers have tapped into popular topics and latched onto popular people to get in front of big Twitter audiences. Their goal: to persuade people to click and visit their Web sites and then hand over personal information, be sold a bill of goods or become infected with a malicious program. The first strategy capitalizes on Twitter users' penchant for searching for random commentary on news subjects. Lately, attackers have been using hundreds of dummy accounts to tweet messages about popular subjects. Links in the messages pointed to malicious video sites pretending to show porn. Visitors who clicked to download a program supposedly needed to watch videos actually installed a fake security application called Privacy Center, which tried to hit them up for money for a full version of the bogus product. Pop culture buzz and shocking breaking news are not the only lures, though. Users should beware any topic that hits Twitter's list of "Trending Topics." The hashtag #smx, used to call out news about a search-marketing conference, reached the list recently and was summarily added to blasts of spam tweets. In a blog post, an irritated conference host said: "We knew this would happen, but it is annoying and becoming a growing problem. Question is, will Twitter do anything about it, beginning with removing its 'Trends' feature?"
Source: http://gadgetwise.blogs.nytimes.com/2009/06/11/more-scamming-and-spamming-on-twitter/

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/.

[Return to top]

Communications Sector

41. *June 11, Victoria Advocate* – (Texas) **Phone service out Wednesday due to cut fiber optic line.** A fiber cut on June 10 left several people in the Crossroads region without phone service. The cut affected both wireless and wireline services, an AT&T spokesman for South Texas said in an e-mail. “The cut was repaired about 1:45 a.m. on June 11, and all service should be running normally for customers,” he wrote on June 11 in the e-mail. It is difficult to determine how many customers were affected by the outage and where the outages took place, the spokesman said, explaining that, with different cables serving different customers, one home could be fine while the home next door loses service. The outage affected customers in the Victoria area, he said, and possibly others in Yorktown and DeWitt County. Other areas most likely remained unaffected.
Source:
http://www.victoriaadvocate.com/news/2009/jun/11/am_phones_061209_54265/?news

[Return to top]

Commercial Facilities Sector

See item **45**

[Return to top]

National Monuments & Icons Sector

42. *June 11, Associated Press* – (Utah) **24 indicted in Four Corners artifact theft probe.** Two dozen people were indicted June 10 after a sweeping undercover investigation into ancient artifacts stolen from public and tribal lands in the Four Corners area. Federal indictments unsealed June 10 accuse the people of stealing, receiving or trying to sell American Indian artifacts, including bowls, stone pipes, sandals, arrowheads, jars, pendants and necklaces. Some 300 federal agents — about half from the Bureau of Land Management — were involved in the arrests of 23 men and women the morning of June 10. Another person has been issued a summons.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5jgv7ro9u1qW4r6ObGV40DSbittFAD98O4N880

43. *June 10, Spectrum* – (Arizona) **Ruby fire slows down.** Cool temperatures and cloud cover are slowing activity on the Ruby Fire eight miles southeast of Tusayan, Arizona. It is approximately 1,300 acres. With the current cool weather and low fire activity, few resources are needed to monitor fire progression. On June 9, resources assigned to the

fire include one engine, one crew, one dozer, archaeologist, resource advisor, an incident commander and operations personnel. The Ruby Fire is 1.5 miles southwest of the Game Reserve Fire in Grand Canyon National Park. Officials from the Kaibab National Forest and Grand Canyon National Park continue to meet on a regular basis to discuss interagency management options for the Ruby and Game Reserve fires.
Source: http://www.thespectrum.com/article/20090610/NEWS01/90610009

[Return to top]

Dams Sector

44. *June 12, Dallas Morning News* – (Texas) **West Dallas homes evacuated after Trinity River pump station fails.** One of the heaviest rainfalls of the season threatened to swamp several West Dallas neighborhoods June 11 after a major floodwater pump station along the Trinity River levees lost power. The Delta pump station — one of six pump stations that move floodwater from outside the levees into the floodway — first lost power around 2 a.m. June 11 and later was struck twice by lightning, causing major damage to its mechanical system. Despite constant work to get it back into operation, the station at Hampton Road and Canada Drive, which can pump up to 90,000 gallons a minute, still was unable to move any water as late as the night of June 11. With the pump station down the next morning, and heavy rain continuing to pour, police officers and firefighters went door-to-door in low-lying neighborhoods around Bickers and Calypso parks, urging people to leave in case floodwater reached houses. By mid-afternoon, the clouds had parted and the rain ceased before homes could be inundated. But at least 60 houses, and perhaps more, were vacated near the pump station and farther east around Sylvan Avenue and Topeka Road, police said. With the Delta pump station down and another set of storms gathering in the west, city emergency crews worked quickly to persuade people in West Dallas to move to higher ground. Delta pump station could require major repairs that will take it out of service for days. The city's entire flood control system depends heavily on its pump stations and a series of sumps made up of channels that snake through the city and of lagoons or ponds that nestle alongside the levees. As of June 12, all six pumps in the system are not up to current standards, the city manager said.
Source: http://www.wfaa.com/sharedcontent/dws/news/localnews/stories/DN-wxpump_12met.ART.State.Edition1.50f6074.html
See also:
http://www.wfaa.com/sharedcontent/dws/wfaa/latestnews/stories/wfaa090611_mo_pumps.7042e8bd.html

45. *June 11, KRCG 13 Jefferson City* – (Missouri) **Workers continue fixing weak dam.** Campers are back, but authorities in Maries County are still monitoring a dam that was damaged on June 11. Some residents and campers of the Turkey Hill Ranch Bible Camp were evacuated when the weak dam on the 40-acre Dudenhoffer Lake almost failed, but was quickly fixed. If the dam, near Freeburg, failed it would have sent water rushing into the Gasconade River, possibly flooding the valley that houses the camp. Maries County Sheriff deputies responded to a report of a damaged spillway at the lake that endangered the safety of the camp's residents. The director of the Turkey camp told

KRCG campers were never in danger during the potential break; many campers were kept on the main grounds of the camp. Crews spent June 10 cutting an emergency spillway for the lake. The problem was two-fold, according to officials. The lake was swollen with rainwater from the previous day's strong storms and that broke the main drain — which was not allowing proper run-off. The dam is now stable and no property was damaged, according to a Maries County sheriff. Crews say there is no imminent danger of a collapse now, but they are still keeping an eye on it.
Source: http://www.connectmidmissouri.com/news/news_story.aspx?id=311810

[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 Website: http://www.dhs.gov/iaipdailyreport

Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
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