Department of Homeland Security Daily Open Source Infrastructure Report for 17 March 2009

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- According to the Associated Press, the Australian government sent a navy mine hunting ship to search Monday for hundreds of tons of chemicals lost overboard during the March 11 freighter mishap that also blackened miles of Australian beaches with fuel oil. (See item **4**)
- DarkReading reports that the Romanian police on March 11 arrested a Romanian resident accused of hacking into several U.S. government servers — including NASA's — and multiple university servers. The hacks on NASA alone cost the space agency some $5 million, according to news reports. (See item **32**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

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 15, USA Today* – (California) **California utility prepares for surge in plug-in electric cars.** Electric cars and plug-in hybrids, which are expected to start hitting the streets next year, could pose a challenge for utilities that are not ready for them. Power companies need to make sure that a concentration of cars in a relatively small area will not overwhelm the grid. Charging has to be safe. Public charging stations need to be considered. Southern California Edison, an investor-owned utility based in the Los Angeles suburb of Rosemead that provides power to 13 million, is trying to get ready. It is spending upwards of $5 million a year acquiring and maintaining the electric vehicle

fleet, testing new plug-ins, and researching battery capabilities.
Source: http://www.usatoday.com/money/industries/energy/2009-03-15-plug-in-electric-cars_N.htm

2. *March 13, Daily Sound* – (California) **Gas leak discovered at Greka facility.** Fire and petroleum investigators conducting a routine inspection of a Greka Energy oil facility near Santa Maria the morning of March 12 noticed the distinctive rotten egg smell of a hydrogen sulfide leak and evacuated the plant, fire officials said. After cordoning off the area, a hazardous materials team isolated the leak, which apparently involved a vapor recovery system. A county fire captain said no injuries or road closures resulted from the incident, which occurred at Greka's Bradley Three Island facility. Inspectors first noticed the smell at approximately 10:30 a.m., he said, and a meter reading showed a dangerous level of hydrogen sulfide gas in the area. Greka workers managed to repair the leak and emergency crews cleared the scene after five and a half hours, authorities said. The chief said the cause of the leak remains under investigation and the oil company will be submitting a failure analysis to the County Fire Department.
Source: http://www.thedailysound.com/News/031309grekagasleak

3. *March 13, Associated Press* – (Montana) **Investigators: People smelled natural gas before Bozeman explosion, didn't report it.** Investigators say a gas leak responsible for leveling a quarter block of downtown Bozeman and killing a woman, was detected in advance by several people, but nobody called to alert authorities. Investigators say a leak in a NorthWestern Energy gas line was behind the explosion on March 5, and it was noticed by people in the area. A Bozeman police detective says investigators learned that, on the morning of the explosion, people did smell gas in the area. But nobody called Northwestern Energy and nobody dialed 911. A Bozeman fire chief says the leak occurred in an underground service line between the main gas line and the meter for Montana Trails Gallery. The victim, a 36-year-old, was working in the gallery at the time of the blast.
Source: http://www.kfbb.com/news/local/41215682.html

[Return to top]

Chemical Industry Sector

4. *March 16, Associated Press* – (International) **Australian navy to help spill clean up.** The Australian government sent a navy mine hunting ship to search Monday for hundreds of tons of chemicals lost overboard during a mishap that also blackened miles of beaches with fuel oil. Authorities said they have scraped the slick off of more than half of the affected beaches just north of the Queensland state capital Brisbane, five days after Wednesday's spillage from the freighter Pacific Adventurer. The spill happened when 31 containers lashed to the ship's deck broke free during a storm and fell overboard, ripping a hole in a fuel tank as they pitched into the sea. Each of the containers held some 22 tons of ammonium nitrate. Authorities say ammonium nitrate dilutes easily in water and that at worst the spilled containers could cause an algal bloom. Still, they should be located and recovered as soon as possible, Australia's environment minister said. The Queensland deputy premier said Sunday an estimated

66,000 gallons of oil spilled from the ship. Britain's Swire Shipping Ltd., the Hong Kong-registered ship's owner, has not publicly confirmed the amount.
Source: http://www.google.com/hostednews/ap/article/ALeqM5hyxN0-euQHg86qF7mqlLLPeUgn-QD96UVS580

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *March 16, Reuters* – (Arkansas) **Entergy shuts Arkansas 2 reactor.** Entergy Corp shut the 995-megawatt Unit 2 at the Arkansas Nuclear One power station in Arkansas from 84 percent power on March 13, the company told the U.S. Nuclear Regulatory Commission in a report. One of the main feed water regulating valves failed causing the steam generator level to lower. That caused operators to shut the reactor.
Source: http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN1647445520090316

6. *March 14, Mid-Hudson News* – (New York) **Federal lawmakers call for investigation of Indian point radioactive leak.** Four Democratic House members have called on the Nuclear Regulatory Commission (NRC) to investigate a recent water leak that contained radioactive material at the Indian Point nuclear power plant in Buchanan. In a letter to the NRC, House members said the leak "demonstrates not only serious deterioration in the physical plant of IPEC but it also calls into question whether IPEC has a program for dealing with its aging infrastructure that is capable of preventing, or even detecting, such deterioration." On February 16, a pipe broke at the facility causing roughly 100,000 gallons of water containing radioactive material to escape, possibly flowing into the Hudson River. The lawmakers said the discharge's source was the nuclear power plant's deteriorating secondary cooling system, which contains the radioactive isotope tritium. The lawmakers said the plant's "physical decline calls into question the wisdom of granting Entergy Nuclear Operations Inc.'s request to extend Indian Point's license for another 20 years beyond the plant's current 40 year license."
Source: http://www.midhudsonnews.com/News/2009/March09/14/IP_leak_reps-14Mar09.html

7. *March 13, Platts* – (Nevada) **NRC issues final regulatory requirement for Yucca repository.** The U.S. Nuclear Regulatory Commission (NRC) issued its final regulatory requirements for a high-level nuclear waste repository at Yucca Mountain, Nevada, on March 13, bringing the agency's rule in line with the radiation dose standard the U.S. Environmental Protection Agency (EPA) issued last year. The NRC rule, which goes into effect April 13, covers the same 1-million-year period, the time after waste has been moved into repository tunnels deep inside Yucca Mountain, as the EPA standard and only addresses changes made in earlier regulations for the post-10,000-year period. NRC adopted the EPA's revised average dose limit of 100-millirem-a-year on radiation escaping the facility. The revision replaces EPA's earlier proposed 350-mrema-year limit for the post-10,000-year period. The NRC left intact the average 15 mrem-a-year radiation dose limit in the EPA standard for the first 10,000 years after emplacement.

Implementation of this rule will mean that NRC has all of its regulatory requirements in place needed to license the Department of Energy's spent fuel disposal facility. The DOE program's ability to more forward, however, is in doubt after the Presidential Administration indicated in a preliminary budget document that the program would only receive enough funds in fiscal 2010, which begins October 1, to answer NRC questions during NRC's licensing review of DOE's application for a Yucca Mountain repository. At the same time, the budget document noted, the United States would be developing a new strategy for managing that waste. The NRC's new rule was published in the Federal Register Friday.
Source:
http://www.platts.com/Nuclear/News/7732109.xml?sub=Nuclear&p=Nuclear/News&?undefined&undefined

[Return to top]

Defense Industrial Base Sector

8. *March 15, Knoxville News Sentinel* – (Tennessee) **More dropsies at the Oak Ridge warhead plant.** It was not exactly like the situation last year, when there were a couple of incidents — barely a week apart — involving dropped warhead components at Y-12. This one, according to a February 20 report by staff of the Defense Nuclear Facilities Safety Board, happened while moving drums containing weapons components. "While moving drums containing weapons components in the Assembly/Disassembly Building, a drum fell from the second level of a stack of drums to the floor (about four feet)," the report said. "The drum fell as a third-level pallet of drums was being removed by forklift. All personnel were appropriately clear of the drums being moved, and the drum had only minor denting on the top and bottom outer edges." The cause of the drop is under evaluation, and B&W, the Y-12 contractor, did not have any information to add to the report, according to a spokeswoman.
Source:
http://blogs.knoxnews.com/knx/munger/2009/03/more_dropsies_at_the_oak_ridge.html

9. *March 14, Santa Maria Times* – (National) **Taurus failure raises Minotaur concerns.** The Air Force is closely tracking the investigation into the recent failure of a Taurus rocket, a sibling to a Minotaur space booster scheduled for liftoff next month from Vandenberg Air Force Base. "The Air Force is participating in the investigation and will determine how the Minotaur systems may be affected," a Space Development and Test Wing representative said. "If it is determined that the Minotaur system is at risk, mitigation efforts will be pursued as appropriate to ensure another failure will not happen." Both the Minotaur and Taurus launch systems are made by Orbital Sciences Corp. Orbital Sciences Corporation as well as NASA are performing a root cause analysis, the results of which will determine if there is a Minotaur 1 and 4 issue. The Taurus and Minotaur systems have some similarity in their designs.
Source: http://www.msnbc.msn.com/id/29691296/

10. *March 14, Denver Post* – (National) **Shuttle launch delays Alliance satellite.** The launch of a military communications satellite by Colorado-based United Launch

Alliance has been delayed until Tuesday. Initially planned for Saturday, the launch of the WGS-2 satellite was pushed back due to rescheduling of the space shuttle Discovery launch for Sunday from Cape Canaveral Air Station, Florida. The satellite is the second installment of the Wideband Global SATCOM system, which will improve communications for U.S. troops.
Source: http://www.denverpost.com/business/ci_11909668

[Return to top]

Banking and Finance Sector

11. *March 16, Berkshire Eagle* – (Maine) **Phone scam targets Greylock Federal's customers.** Dozens of Greylock Federal Credit Union members were targeted by a phone scam recently, but very few fell prey to the illegal solicitation, according to credit union officials. The senior vice president said the "vast majority" of customers contacted were not victimized by the pre-recorded message, claiming to represent Greylock Federal, that was sent throughout Berkshire County starting on March 14 and ending on March 15. The senior vice president could not say how many of the credit union's 65,000 members received the phone call, but it was far greater than the nearly 70 Pittsfield residents city police said called them to complain about the scam. The message was seeking vital credit card information, such as account and pin numbers, to verify an alleged claim of fraudulent purchases against that person's credit card. Once Greylock Federal was notified of the scam, the senior vice president said the financial institution put out an alert to its weekend answering service and called in staff members to deal with customers who still had concerns, or actually gave out their credit card numbers.
Source: http://www.berkshireeagle.com/ci_11923291

12. *March 13, DarkReading* – (International) **Major cybercrime busts take place in Romania.** The Romanian police on March 11 broke up a major bank fraud ring. According to news reports, the Romanian police, working along with the FBI, arrested 20 individuals who allegedly built cloned bank sites and then drained the accounts of users who were lured into logging in to them. The cloned sites, which were deployed in Italy and Spain, looked and operated like the actual bank Web sites, but they asked users questions that ultimately led to the divulging of personal bank details, according to the chief of the Romanian police's organized crime division. Once obtained, the hackers allegedly used that information to access the real bank Web sites and transfer or withdraw cash. Nearly 100 police officers from special troops entered suspects' houses in major cities across Romania, the reports said. Investigators said the ring stole at least 350,000 euros.
Source:
http://www.darkreading.com/security/cybercrime/showArticle.jhtml;jsessionid=55MMQXQOXACUEQSNDLRSKH0CJUNN2JVN?articleID=215900249

13. *March 13, Holland Sentinel* – (Michigan) **Credit union closed as canine unit searches for 'suspicious threat.'** Ottawa County sheriff's deputies investigated what they called a "suspicious threat" at a credit union in Holland Township on March 13. Deputies were called to Nu Union Credit at 10:24 a.m., and they evacuated the building. The credit

union remained closed for two hours while deputies and a canine unit searched the premises, but the search turned up nothing, a sergeant of Ottawa County Sheriff's Office said. A manager at the credit union refused to say if the reported threat involved a robbery or a weapon. No one was injured in the incident, he said.
Source: http://www.hollandsentinel.com/news/x679797639/Credit-union-closed-as-canine-unit-searches-for-suspicious-threat

14. *March 13, Bank Technology News* – (International) **Visa: two firms noncompliant.** Visa Inc. has pulled Heartland Payment Systems Inc. and Royal Bank of Scotland Group PLC's RBS WorldPay from its list of companies that comply with the Payment Card Industry data security standards. Heartland and RBS WorldPay will stay off the list until the two processors close the holes that led to the massive data breaches reported in January and December, Visa said on March 13 in an e-mail. "Visa will consider relisting both organizations following their submissions of their PCI DSS reports on compliance," the San Francisco company said. Both continue to handle Visa transactions. Heartland has said it met the standards when its systems were last assessed in April. On March 13 it said it is undergoing a PCI assessment, which it expects to complete by May "and will result in Heartland, once again, being assessed as PCI-DSS compliant." WorldPay said in an e-mail statement on March 13 it expects its assessment to be complete by the end of April. "Because of the criminal intrusion, we need to be recertified earlier than the normal schedule." Visa has voiced support for the PCI standards, saying they remain "an effective security tool when implemented properly" and "the best defense for businesses against the loss of sensitive data." After Heartland disclosed its breach, its chief executive called for the industry to move to end-to-end encryption and for companies to share information about specific incidents. The American Bankers Association has advocated that other payment companies be subject to the Gramm-Leach-Bliley Act risk-based standards that banks must follow.
Source: http://www.americanbanker.com/btn_article.html?id=20090313F6IR46WE

[Return to top]

Transportation Sector

15. *March 16, Associated Press* – (Louisiana) **Flight lands safely in New Orleans after bird hit.** A Delta Air Lines plane has landed safely in New Orleans after striking a bird shortly after takeoff. A spokeswoman for Louis Armstrong New Orleans International Airport said Delta Flight 1053 returned to the tarmac shortly after takeoff on its flight on the morning of March 16. The plane had been bound for Atlanta. Another spokeswoman said passengers were booked on other flights. She was told there were about 191 people on board.
Source: http://www.google.com/hostednews/ap/article/ALeqM5jiUHjnFAfmy-LFaUVhZQYg52f7RwD96V7GL80

16. *March 16, Baltimore Examiner* – (Maryland) **Charles Street bridge demolition to begin tonight.** Construction will begin March 16 on a more than $50-million dollar project to rebuild the Charles street bridge overpass above the beltway in Towson. Authorities say the bridge is more than 50-years old and that it is structurally deficient.

In a press release, the Maryland State Highway Administration says the work will help in the future widening of the Baltimore Beltway and will lead to major changes in traffic patterns on Charles Street and I-695. Authorities say construction will make the bridge wider, longer, and higher and could eventually be added to I-695. Crews will also help rehabilitate the light rail line in the Towson area. During construction, motorists can expect temporary lane closures and possible prolonged ramp closures. Officials say drivers should use I-83 or York road as alternates. Construction is expected to last through the fall of 2012.
Source: http://www.examiner.com/x-5506-Baltimore-Traffic-Examiner~y2009m3d16-Charles-street-bridge-demolition-to-begin-tonight

17. *March 15, Reno Gazette Journal* – (Nevada) **Mercury spill closes 1 gate at Reno-Tahoe International.** A Southwest Airlines passenger jet at Reno-Tahoe International Airport was grounded for several hours at the gate on March 15 as the result of a mercury spill from a blood-pressure monitoring device. No injuries were reported, and cleanup was under way. A female passenger with the blood-pressure device in her carry-on bag was getting off the plane that had arrived from Seattle about 12:30 p.m. March 15, an airport spokesman said. "Apparently somehow it had broken...and it had leaked mercury into the aircraft..." said the spokesman. The mercury also spilled onto some of the jet bridge connecting the terminal to the 737. One gate was closed at Reno-Tahoe International. "Everything else is fully operational and functioning," said the spokesman. No passengers remained on the plane. The airport fire department was contacted; its hazardous materials-trained team arrived, and sealed off the area and the jet bridge. A preliminary clean up was carried out. Later, a private environmental company was planning a "thorough, in-depth cleanup of the area and monitoring of the air quality inside that jet bridge, before they clear that area to be open to the public again," said the spokesman.
Source: http://www.rgj.com/article/20090315/NEWS18/90315020/1321/news

18. *March 13, Associated Press* – (National) **Post-9/11 reforms do not stop passport fakery.** Using phony documents and the identities of a dead man and a 5-year-old boy, a government investigator obtained U.S. passports in a test of security after the September 11th attacks. Despite efforts to boost passport security since the 2001 terror attacks, the investigator fooled passport and postal service employees four out of four times, according to a new report made public March 13. The report by the Government Accountability Office, Congress' investigative arm, details the ruses: One investigator used the Social Security number of a man who died in 1965, a fake New York birth certificate and a fake Florida driver's license. He received a passport four days later; a second attempt had the investigator using a 5-year-old boy's information but identifying himself as 53 years old on the passport application. He received that passport seven days later; in another test, an investigator used fake documents to get a genuine Washington, D.C., identification card, which he then used to apply for a passport. He received it the same day; a fourth investigator used a fake New York birth certificate and a fake West Virginia driver's license and got the passport eight days later. Criminals and terrorists place a high value on illegally obtained travel documents, U.S. intelligence officials have said. Currently, poorly faked passports are sold on the black market for $300, while

top-notch fakes go for around $5,000, according to Immigration and Customs Enforcement investigations. The State Department has known about this vulnerability for years. On February 26, the State Department's deputy assistant secretary of passport services issued a memo to Passport Services directors across the country stating that the agency is reviewing its processes for issuing passports because of "recent events regarding several passport applications that were approved and issued in error." Source: http://washingtontimes.com/news/2009/mar/13/post-911-reforms-dont-stop-passport-fakery/

[Return to top]

Postal and Shipping Sector

19. *March 14, KOB 4 Albuquerque* – (New Mexico) **Bank receives envelope with white powder.** A threatening letter containing white powder forced the evacuation of a bank in northeast Albuquerque on March 13. AFD and HAZMAT responded to the Bank of the West near San Pedro and Menaul. About six employees were cleared from the building. A spokesperson for the Postal Inspector, whose office is handling the investigation, said the letter was addressed to the president of the bank. An employee opened the letter, and white powder fell out. The powder is non-hazardous but since there was an "undisclosed" threat in the letter, the FBI and post office will be investigating who sent it and what charges could be filed. Officials said they do not think the letter is a biohazard. However, they are taking precautions to be sure.
Source: http://www.kob.com/article/stories/S831301.shtml

[Return to top]

Agriculture and Food Sector

20. *March 16, USAgNet* – (National) **USDA bans slaughter of downer cattle.** The Agriculture Secretary announced a final rule to amend the federal meat inspection regulations to require a complete ban on the slaughter of cattle that become non-ambulatory disabled after passing initial inspection by Food Safety and Inspection Service (FSIS) inspection program personnel. The final rule amends the federal meat inspection regulations to require that all cattle that are non-ambulatory disabled cattle at any time prior to slaughter at an official establishment, including those that become non-ambulatory disabled after passing ante-mortem inspection, be condemned and properly disposed of according to FSIS regulations. CattleNetwork.com reports that the final rule requires that establishments notify inspection program personnel when cattle become non-ambulatory disabled after passing the ante-mortem, or pre-slaughter, inspection. The rule will enhance consumer confidence in the food supply and improve the humane handling of cattle. Under the final rule, cattle that become non-ambulatory disabled from an acute injury after ante-mortem inspection will no longer be eligible to proceed to slaughter as "U.S. Suspects." Instead, FSIS inspectors will tag these cattle as "U.S. Condemned" and prohibit these cattle from proceeding to slaughter. Discontinuing the case-by-case disposition of cattle that become non-ambulatory disabled after ante mortem inspection will eliminate the time FSIS Public Health Veterinarians spend

conducting additional inspections on these animals, thereby increasing the time inspection program personnel can allocate to other inspection activities.
Source: http://www.usagnet.com/story-national.php?Id=589&yr=2009

21. *March 16, Los Angeles Times* – (National) **Checkout alert system for recalled foods sought.** With more food recalls happening weekly, consumer advocates, supermarket chains and legislators are exploring better ways to stop the sale of tainted food, and one plan under discussion by lawmakers in Sacramento involves using supermarket checkout scanners to help. Programming supermarket computers to trigger an alert every time a recalled product is scanned at the checkout counter could be an easy way to better protect shoppers from buying and eating tainted foods, consumer groups say. Although the influential California Grocers Association is taking a wait-and-see stance on the proposal, some major retailers already are exploring the idea themselves. Cincinnati-based Kroger Co., which operates 260 Ralphs and 118 Food for Less stores in California, has programmed its computers to issue a "hard halt" to any transaction involving a recalled product. Ralphs also uses its so-called loyalty-reward cards, which track a holder's purchases, to warn participating customers via a notice on their sales receipt that they might have recalled and possibly dangerous foods sitting in their pantries. Costco Wholesale Corp. tentatively supports the checkout alert system and "anything we can do to protect the consumer," said the assistant vice president for food safety and quality assurance of the Issaquah, Washington-based warehouse chain.
Source: http://www.latimes.com/business/la-fi-recall16-2009mar16,0,5315194.story

22. *March 13, WVLT 8 Knoxville* – (Tennessee) **Fire erupts Friday afternoon at East Tennessee corn refinery plant.** A fire ignited Friday afternoon around 2:30 p.m. at the Tate and Lyle corn refinery plant in Loudon, according to Loudon Police. A Loudon City Police chief said the fire in one of the plant's smokestacks is under control and no one was injured. The plant was shut down for scheduled four to six week maintenance period at the time of the blaze, according to a Tate and Lyle spokesman. Officials say a stray spark from a cutting tool ignited in a take of liquid fiberglass. The plant was evacuated while firefighters battled the flames from a ladder truck. According to the company's Web site, the Loudon plant refines corn for animal feed, cereal sweeteners, ethanol, and food starches.
Source: http://www.volunteertv.com/news/headlines/41224942.html

23. *March 13, U.S. Food and Drug Administration* – (New York) **Asia cash and carry recalls Crown Farms Brand "Gulsha" fish because of possible health risk.** Asia Cash & Carry Inc. in Maspeth, New York is recalling 17 cases of Crown Farms brand "GULSHA" Frozen Fish (Bangladeshi Freshwater Fish) in 500g packages with production code AUG 2008 because the product has the potential to be contaminated with salmonella. Crown Farms brand "GULSHA" (Bangladeshi Freshwater Fish) Fish was distributed to retail stores in New York, New Jersey, Illinois, Michigan, and Virginia. The GULSHA Frozen Fish was imported from Bangladesh, and distributed in cases containing vacuum-packed 500g packages with a production date of August 2008, expiration date July 2010, and UPC code 5 060065 430704. There are 16 - 500g packages per case. No illnesses have been reported to date. The recall is the result of

sampling by the U.S. Food and Drug Administration (FDA) which revealed that the finished product contained the bacteria. The company had partially distributed the entry prior to FDA's findings.
Source: http://www.fda.gov/oc/po/firmrecalls/asiacash03_09.html

24. *March 13, U.S. Food and Drug Administration* – (New York) **Peregrina Cheese Corporation recalls queso fresco because of possible health risk.** Peregrina Cheese Corporation of Brooklyn, New York is recalling one code of its 14-ounce packages of Queso Fresco Fresh Cheese Mexican style soft cheese because they have the potential to be contaminated with Listeria monocytogenes. The recall cheese was distributed to retail stores in New York City (Brooklyn, Queens, Bronx and Manhattan) and Pennsylvania (Scranton and Hazelton). The Queso Fresco Fresh Cheese comes in a 14 ounce foil wrapped package marked with code 4483, UPC 8 17424 00024 6, and bearing Plant # 36-8431. The cheese was produced on February 18, 2009. No illnesses have been reported to date. This recall is the result of sampling and analysis by the U.S. Food and Drug Administration which revealed that finished product contained the bacteria.
Source: http://www.fda.gov/oc/po/firmrecalls/peregrina03_09.html

[Return to top]

Water Sector

25. *March 15, Newsday* – (New York) **Toxins from old Grumman site contaminating Bethpage.** Recent tests showed elevated levels of the industrial solvent trichloroethylene — a potential carcinogen also known as TCE — in the basements of four homes east of the Navy-owned property's 11th Street boundary in Bethpage, New York. Contaminated soil vapor was also found under the basement slabs of two more houses. Navy investigators have given residents carbon air filters to reduce TCE vapor levels immediately. They plan to install systems to vent gases from homes where concentrations exceed state indoor air standards. The problem appears to be limited to a roughly two-block area. The news has unsettled residents, who are dubious of the Navy's assurance that the state health guideline for TCE levels indoors — 5 micrograms per cubic meter of air — is set many times lower than levels that cause health effects. It is the latest toxic legacy from the 635-acre former defense plant. Among them: a plume of contaminated groundwater containing TCE that has moved south from two hazardous-waste sites. It has spread nearly two miles wide and is headed for public drinking water wells. In the most recent case, the pollution came from leaking drums of volatile chemicals stored decades earlier on a four-acre portion of the site. An earlier cleanup effort that ended in 2002 removed more than 2 tons of chemicals from soil and groundwater. But small pockets of tainted soil gas remained, allowing vapor to seep back up through the soil and into some homes — a process known as vapor intrusion.
Source: http://www.newsday.com/news/printedition/longisland/ny-livapo146070171mar15,0,6508924.story

26. *March 15, WTVT 13 Tampa* – (Florida) **Running out of water.** The C.W. Bill Young Reservoir covers 1,100 acres and can hold up to 15 billion gallons of water. Managers say it has run dry. "From a water supply standpoint, it is, in effect, empty," according to

the Tampa Bay Water general manager. The reservoir is supposed to be a major source of drinking water for the Bay Area. The fact that it is dry should come as no surprise. Late last month, the executive director of the Southwest Florida Water Management District made a prediction, "This is an extreme water shortage. The Bill Young Reservoir is going to be empty in two or three weeks. Our two major rivers are at historic lows for this time of year." He made that prediction shortly after the SWFWMD board voted against imposing Phase 4 water use restrictions. The request for tougher water use rules came from Tampa Bay Water. Had Phase 4 been imposed, it could have banned most, if not all, residential lawn watering. Current rules limit lawn watering to just one day a week. The SWFWMD board opted to toughen existing rules, which focused more on enforcement after landscapers and sod farmers complained about the consequences of Phase 4.
Source:
http://www.myfoxtampabay.com/dpp/news/local/hillsborough/Reservoir_dry_031509
See also: http://www.tampabay.com/news/environment/water/article983732.ece

27. *March 14, Wisconsin State Journal* – (Wisconsin) **State might insist all municipalities treat drinking water.** All municipalities in Wisconsin would have to disinfect their drinking water under rules being written by the state Department of Natural Resources (DNR). The new groundwater rules are being driven not only by a change in federal regulations but also by recent research that shows numerous public wells in the state contaminated by viruses. While the majority of the state's municipalities already treat drinking water, the new rules will affect more than 70 communities throughout the state that currently pump untreated water. Among those communities in southern Wisconsin, according to the DNR, are Spring Green, Mineral Point, Hollandale and Dane. Nearly all large cities such as Madison treat drinking water with chlorine or through some other process. The rules will be presented to the Natural Resources Board sometime this summer, according to the head of the DNR's public drinking water section. Public hearings would be held before the rules are returned to the board for a final vote, he added. While the rules would affect mostly those communities that would have to install treatment systems, the science behind the change — the presence of viruses in deep municipal wells and recent studies that show related human health impacts — has created a new awareness that even drinking water taken from deep underground aquifers is a fragile resource and surprisingly susceptible to contamination. The groundwater rules are being rewritten to comply with changes in federal groundwater rules from the Environmental Protection Agency (EPA), he said. Those federal rules will require stricter monitoring of contaminants such as viruses and bacteria. They would not require disinfection at all water systems. But he said recent research has shown that even when testing turns up no indicators of possible viral contamination, such as the presence of E. coli bacteria, further tests have still revealed viruses. That uncertainty, he said, has prompted the DNR to propose going beyond the EPA rules and require treatment by all municipal drinking water systems.
Source: http://www.madison.com/wsj/topstories/442975

[Return to top]

Public Health and Healthcare Sector

28. *March 16, Associated Press* – (District of Columbia) **HIV-AIDS rate in D.C. 'higher than West Africa.'** At least 3 percent of residents in the nation's capital are living with HIV or AIDS and every mode of transmission is on the rise, according to a report to be released Monday by D.C. health officials. The findings in the 2008 epidemiology report by the D.C. HIV/AIDS Administration point to a severe epidemic that is impacting every race and sex across the population and neighborhoods. "Our rates are higher than West Africa," said the administration's director, who used to spearhead the Centers for Disease Control and Prevention's work in Zimbabwe. "They're on par with Uganda and some parts of Kenya." The study found that the number of HIV and AIDS cases jumped 22 percent from the 12,428 reported in 2006. Almost 1 in 10 residents between 40 and 49 are living with the virus.
    Source: http://www.foxnews.com/story/0,2933,509316,00.html

29. *March 15, Associated Press* – (International) **Passenger on Frankfurt-to-Detroit flight had TB.** The Centers for Disease Control and Prevention says a passenger on a Northwest Airlines flight from Frankfurt, Germany, to Detroit has been diagnosed with tuberculosis. Northwest says the passenger was on Flight 51 on March 12 to Detroit Metropolitan Airport. A CDC spokeswoman said the risk is low that other passengers might contract tuberculosis. She said Sunday that health officials were seeking to contact 17 passengers seated near the sick passenger so they can be tested for tuberculosis as a "cautionary move."
    Source: http://www.washingtonpost.com/wp-dyn/content/article/2009/03/15/AR2009031501182.html

[Return to top]

Government Facilities Sector

30. *March 14, Associated Press* – (Colorado) **Man accused of bomb threat at Buckley air base.** A Boulder man has been indicted on a federal charge of phoning a bomb threat to Buckley Air Force Base in suburban Denver. The suspect was indicted on March 11 and arrested on March 13. The 27-year old suspect faces a sentence of up to 10 years in prison and a fine of up to $250,000 if convicted. Prosecutors say the bomb threat was phoned to Buckley on January 21.
    Source: http://cbs4denver.com/crime/Bomb.Threat.Buckley.2.959416.html

31. *March 14, Spamfighter* – (New York) **Computer virus snapped networks at Sullivan government offices.** A dangerous virus that infected computers of the Sullivan County Government Center as well as those in the Sheriff's Office in Monticello has paralyzed the networks of both the institutions. Security investigators suspect that the virus emerged from the Netherlands and crept in so quietly that antivirus software could not detect it when it infected the county's computers. The manager at Sullivan County said that due to the virus attack, a whole week's productivity was lost, as reported by recordonline on March 5, 2009. The investigation is focused on whether there is any

other channel like a portable device through which the virus might have entered the District Attorney's or Sheriff's Office computers.
Source: http://www.spamfighter.com/News-11997-Computer-Virus-Snapped-Networks-at-Sullivan-Government-Offices.htm

32. *March 13, DarkReading* – (International) **Major cybercrime busts take place in Romania.** The Romanian police on March 11 arrested a Romanian resident accused of hacking into several U.S. government servers — including NASA's — and multiple university servers. The hacker had set up several servers in the United States, which he controlled from Romania and used to carry out the hacks, according to reports. The hacks on NASA alone cost the space agency some $5 million, according to news reports. The accused attacker has previously been accused of breaking into computers at the U.S. Navy and Department of Energy between 2005 and 2006. The accused attacker reportedly said he made the hacks only to prove vulnerabilities in the key government systems, and that he did not expect to make any material gains. However, NASA was forced to rebuild its systems and temporarily had to change over to manual communications when the hack was discovered. He previously was indicted for his alleged participation in a hacker group called the "Whitehat Team," whose goal was to break into the most secure systems in the world. U.S. authorities have claimed $2 million in damages from the attack. He was charged with breaking into government computers last November. He has been indicted on 10 counts, including charges of conspiracy, unauthorized access to government computers, and causing intentional damage to computers. He will be brought to Los Angeles for trial after his Romanian proceedings conclude, authorities said.
Source:
http://www.darkreading.com/security/cybercrime/showArticle.jhtml;jsessionid=55MMQXQOXACUEQSNDLRSKH0CJUNN2JVN?articleID=215900249

33. *March 13, WSB 750 Atlanta* – (Georgia) **Charges expected in Dobbins incident.** A 29 year old transient from Indiana is expected to face charges in connection to the March 12 standoff outside the front gate at Dobbins Air Reserve Base in Cobb County. The suspect is undergoing psychiatric evaluations at Northwest Regional Hospital. An Air Force spokesman said that the suspect raised suspicions when he approached the guard gate, said he had something dangerous in his car and, "felt funny." Traffic on Highway 41 was tied up for hours as a police robot checked the car. A propane tank and a loaded shotgun were found inside.
Source: http://wsbradio.com/localnews/2009/03/charges-expected-in-dobbins-in.html

34. *March 13, Cookeville Herald-Citizen* – (Tennessee) **Two juveniles remain held for pipe bomb.** Two 13-year-old Monterey boys are being held in the Putnam Juvenile Detention Center on charges relating to a pipe bomb found at Burks Middle School in Cookeville on March 11. The two were taken into custody on March 11, and on March 12 at a brief hearing in Juvenile Court the presiding judge ordered that they will continue to be in custody pending a bond hearing during the week of March 16-20. One of the boys is charged with possession of a weapon on school property and possession of the components to make an explosive device. The other boy is charged with possession

of a weapon on school property. Though the case is still under investigation and officers working on it have declined to discuss it, it appears that one boy made the device and took it to school to give to the other boy, who then took it home with him. Apparently, the device, which has been described as a cylinder-shaped object wrapped in black tape with a fuse hanging out, had been at the school earlier in the day unknown to anyone other than the two boys. So far, there has been no allegation of any threat or intent to explode the "bomb" at the school.
Source: http://www.herald-citizen.com/index.cfm?event=news.view&id=00AC1D2A-19B9-E2E2-67A207232B945196

35. *March 13, Arizona Republic* – (Arizona) **Warrants to search Agua Fria sites issued in mercury spill.** Avondale police on March 12 served warrants to search three Agua Fria Union High School District sites in connection with a mercury spill. It is the latest development in the investigation into the February 12 toxic spill at Agua Fria High School. The district spent close to $150,000 after the spill and shut down the school for three days, documents show. The final cost will "be fairly expensive," the assistant superintendent said. District officials refuse to say how the mercury got on the campus or how it was spilled, but district e-mails obtained by the Arizona Republic show a student "had taken the mercury from these classrooms" at Agua Fria High School. Police warrants seek documents and evidence related to the probe. The warrants were served at the school, district office, and a building which houses the information technology department.
Source: http://www.azcentral.com/news/articles/2009/03/13/20090313swv-mercury0314.html

[Return to top]

Emergency Services Sector

36. *March 16, WBRZ 2 Baton Rouge* – (Louisiana) **BR implements telemedicine program.** Baton Rouge on March 12 became the second city in the United States to implement a telemedicine program that allows doctors to treat patients en route to the emergency room, city-parish officials said. Initially, the specially equipped ambulance will communicate only with Our Lady of the Lake Regional Medical Center, but plans call for the program to be expanded to all seven major area hospitals with federal Homeland Security funds, said the assistant director of Emergency Medical Services. Our Lady of the Lake was selected for the pilot program because it already uses a hard-wired telemedicine system to monitor intensive-care patients from a central location, he said. The ambulance in the "BR Med-Connect" program will use the same wireless mesh network that police are using for their new high-tech surveillance system, which includes not only video cameras but shot-spotters that detect the origin of gunshots. The city-parish program consists of one ambulance equipped with $25,000 worth of equipment. When linked to another $30,000 in equipment at a hospital, the system will allow doctors not only to see and communicate with EMS patients, but also to monitor data from diagnostic machines.
Source: http://www.2theadvocate.com/news/41190372.html

37. *March 15, WHAS 11 Louisville* – (Kentucky) **Newest unit of Kentucky National Guard activated.** The newest unit of the Kentucky National Guard is now activated and ready to respond to emergencies. Some have already helped during the ice storm. The unit is described as an airbase in a box. The 123rd Contingency Response Group will be an early-responder in the event of terrorist attacks, natural disasters, or other major emergencies within a 400 mile radius of Louisville. The group is made up of airmen who were already members of the Kentucky Air National Guard, many of whom were put in to action in the icy conditions in late January. The unit is comprised of 115 Kentucky Air National Guard members.
Source:
http://www.whas11.com/news/local/stories/whas11_localnews_090315_NationalGuard.3b2192c1.html

[Return to top]

Information Technology

38. *March 16, Computer Business Review* – (International) **Egress addresses data loss with secure exchange.** A new data exchange system that will secure information wherever it is sent as an email attachment, by file transfer, or on a CD, DVD, or USB stick could finally put an end to breaches after data is forwarded in error, stolen, or lost in the post. Launched on March 16 by Egress Software Technologies, Switch uses encryption and a Web-based policy engine to enforce security rules on files before and after they are shared. "Switch uses strong AES 256-bit encryption and builds a secure package around files to be shared," the president of US Operations said. "It assigns an identity to each package and applies real-time controls on what a recipient can do with a file that is shared with them." "We believe it is a very important aspect of security that is under-served. We have done a lot of research in the market and found that although there are plenty of different secure messaging offerings, they each only address a piece of the puzzle." He said the company had considered the various merits of file and full disk encryption, PKI and EDI, data leakage, and enterprise rights management software before deciding on a strategy for Switch. "With Switch we wanted to develop a system that would enforce the same strong security policies as are used internally, to the business of sharing sensitive data with people outside the perimeter" the president said. He explained that the system does not interfere with business processes in any way, so a file can go out by a courier on a disc, or sent across an FTP network. Either way, it is secured by Switch's 'follow-the-data protection.'
Source:
http://www.cbronline.com/news/egress_addresses_data_loss_with_secure_exchange_160309

39. *March 13, IDG News Service* – (International) **Foreign Web attacks change security paradigm.** Traditional security systems may be ineffective and become obsolete in warding off Web attacks launched by countries, according to the founder of Attack Research. New attack trends include blog spam and SQL injections from Russia and China, he said during his talk at the Source Boston Security Showcase on March 13. "Client-side attacks are where the paradigm is going," the founder of Attack Research

said. “Monolithic security systems no longer work.” Hackers use Web browsers as exploitation tools to spread malware and collect sensitive information. The founder of Attack Research used examples from clients of his company, which analyzes and researches computer attacks, to demonstrate the threat posed by blog spam and SQL attacks. Attackers targeted high-traffic sites with blog spam and posted comments on blogs, he said. The comments looked odd and tended to have non-English phrases placed in large blocks of text with random words hyperlinked, he said. Clicking on such links took users to sites that seemed like blogs but were pages loaded with malware, he said. A Chinese bank owned the domains for each malware site, but the IP (Internet Protocol) addresses traced to Germany. Studying the links revealed that each one contained words in Russian or Romanian, said the founder of Attack Research. By placing an international spin on their nefarious activities, the hackers hoped to confuse anyone investigating their work, he said.
Source:
http://www.pcworld.com/businesscenter/article/161247/foreign_web_attacks_change_security_paradigm.html

40. *March 13, Softpedia* – (International) **Windows server man-in-the-middle attack vulnerability is patched.** On March 10, Microsoft released three security bulletins designed to deal with vulnerabilities in Windows client and server platforms. Security Bulletin MS09-008 rated Important is focused on patching issues in DNS and WINS Server impacting Windows 2000 Server, Windows Server 2003, and Windows Server 2008. The past week, Microsoft dismissed claims that MS09-008 did not actually patch the DNS Server Vulnerability in WPAD Registration Vulnerability- CVE-2009-0093. MSRC Engineering and Windows Core Networking made available documentation describing in detail the security holes associated with MS09-008 and the updates made available by Microsoft. “There are claims that this update is ineffective. Let me be clear that this update will protect you and it should be deployed as soon as possible. Below is an overview on how the complete security update helps protect a system,” an analyst of MSRC Engineering stated. The Response Communications, MSRC, manager also dismissed the possibility of MS09-008 being ineffective. He indicated that Microsoft managed to review all the feedback it received, and ensured Windows Server customers that deployed the security bulletin that they were indeed protected against attacks targeting the vulnerabilities patched via MS09-008. The software giant informs that it is now aware of any attacks targeting security holes plugged by MS09-008.
Source: http://news.softpedia.com/news/Windows-Server-Man-in-the-Middle-Attack-Vulnerability-Is-Patched-106865.shtml

41. *March 13, SoftPedia* – (International) **Exploit for Foxit Reader flaw released.** Several serious vulnerabilities affecting the Adobe Reader alternative, developed by Foxit Software, have been recently disclosed. Security professionals now warn that proof-of-concept (PoC) exploit code for one of the more critical ones has also been made available and could be used in future attacks. On March 9 Foxit released security updates for its Reader product versions 3.0 and 2.3. As explained in the accompanying advisory, these addressed three serious flaws reported by CORE Security and Secunia, two vulnerability research companies. One of the bugs reported by CORE was

categorized as a stack-based buffer overflow and allowed an attacker to run commands or execute files by tricking a potential victim into opening a maliciously-crafted PDF file. A programmer identifying himself as "SkD" has made available a fully-working exploit for this vulnerability. According to the code comments, he has written the PoC for Windows XP SP3 and it is based on information published by CORE. This is particularly interesting, because it means that users of the two most popular PDF reading applications for Windows, Adobe Reader and Foxit Reader, are now susceptible to attacks at the same time. As previously reported, a similar arbitrary code execution vulnerability in Adobe Reader 9 and earlier has been actively exploited in the wild. Adobe released a patch for the flaw affecting its Adobe Reader and Acrobat products only recently, on 10 March, almost three days after it was reported as a 0-day. Even so, the patch is only available for version 9 of the products, users of earlier versions being required to upgrade first. Because the vulnerability made the subject of active attacks and initially suggested workarounds like disabling JavaScript did not help much, some people recommended switching to Foxit Reader, which now does not sound like such a great solution either.
Source: http://news.softpedia.com/news/Exploit-for-Foxit-Reader-Flaw-Released-106739.shtml

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

Nothing to report

[Return to top]

Commercial Facilities Sector

42. *March 15, WJW 8 Cleveland* – (Ohio) **Carbon monoxide scare sends nearly 100 to the hospital.** A Gates Mills, Ohio hockey arena was evacuated after a carbon monoxide (CO) scare over the weekend. Nearly 100 people were taken to area hospitals for treatment after experiencing symptoms of CO poisoning. The Gilmour Academy in Gates Mills had been hosting the ACHA National Championship tournament. Around 8 o'clock on March 14, two of the games were canceled after firefighters detected high levels of carbon monoxide. By March 16, the problems had been corrected and the tournament was back on the ice. According to the Gates Mills Fire Department, the carbon monoxide back-up was caused by a number of reasons. The machines that smooth the ice were not functioning properly. The ventilation system was not supplying sufficient outside air. And the team buses were running close to the fresh air intake of

the arena. Everyone has been treated and released from the hospital.
Source: http://www.fox8.com/news/wjw-coscare,0,7411840.story

43. *March 15, WJZ 13 Baltimore* – (Maryland) **Police search for suspects in Walmart bomb case.** Deputy State Fire Marshals and officers with the Elkton Police Department are continuing their investigation into the detonation of a destructive device at the Super Walmart store in Elkton on March 14. Investigators recovered evidence from the men's restroom after the device (commonly known as a soda bottle bomb) was set off. At the time of the explosion a middle age man was using the restroom and a small child just walked out. Surveillance cameras monitoring the parking lot and inside the store captured four males walking into the store and walking directly into the men's restroom at approximately 9:07 p.m. The individuals were later observed walking through the store after the explosion. It is believed one of the men has been involved in two other similar incidents at the store within the past several weeks. Authorities are seeking the public's help in identifying these individuals. The construction of these devices has been mischaracterized as a prank, however, the destructive effect and the potential of serious injury is extremely high.
Source: http://wjz.com/local/bomb.walmart.2.959711.html

44. *March 13, Associated Press* – (Oklahoma) **Report: High winds could topple Norman building.** An empty six-story building in downtown Norman has been found to be structurally unsound and could be brought down by a 50-mile-per-hour wind gust. City officials have developed a plan to evacuate the area around Financial Center Building and create a "clear zone" in case of high winds or approaching storms. The building's owner hired an engineering firm to assess its structural integrity after several cracks were discovered. At that time the building's tenants such as Vista Restaurant and several law firms voluntarily vacated the building. The owners now have a city permit to begin a temporary stabilization project and the work is scheduled to begin March 15 and take eight weeks to complete.
Source: http://www.kswo.com/Global/story.asp?S=10002104

[Return to top]

National Monuments & Icons Sector

Nothing to report

[Return to top]

Dams Sector

45. *March 15, WJBF 6 Aiken County* – (South Carolina) **Dam breaks, threatens road in Johnston, SC.** Crews are setting up a second pump. A man working on the repair said, "We're just putting some extra pipe down, trying to get more water away from the hole, trying to relieve a little pressure on it, keep it from washing the road out." The dam is actually what cars drive over. Holmes Pond Rd. runs on top of it, and on the night of March 12, part of the dam caved in. A WJBF reporter said, "What's happened here is

the excess water has come over here where the dam has broken. It's beginning to erode this side, causing a sinkhole, and it's boring its way underneath this road here. It's coming to the other side, causing this side of the road to cave in, and the next thing to go, could be the road itself." The worker said, "Not real sure what happened yet. Apparently it has washed out a portion of the dam, it has not washed completely through yet, ruining the road, but that's what we're trying to prevent." Two pumps are sucking out 1,000 gallons a minute, but crews have a sinking feeling the rain is not on their side. So to make sure the sinkholes stop here, crews are working around-the-clock, to get water out, even while it keeps pouring in. Crews there told WJBF they expect the road to be closed for at least another week while they continue to work on the problem.
Source:
http://www.wjbf.com/jbf/news/state_regional/south_carolina/article/dam_breaks_threatens_road_in_johnston_sc/11850/

46. *March 15, Seattle Times* – (Washington) **South King County at high risk for flooding.** Four South King County cities face their most serious flooding risk in 40 years next fall and winter because of January damage to a flood-control dam on the Green River, authorities have warned. The Army Corps of Engineers, which built and maintains the Howard Hanson Dam, says it does not know what caused a 10-foot-wide, 6-foot-deep depression in an abutment to the rock and earthen dam. As a safety precaution, the Corps will store less water behind the dam until engineers can figure out what caused the problem in the reservoir wall adjoining the spillway — and how to fix it. In the meantime, the Corps will be forced to release into the lower Green River essentially all rainwater from storms, and risk overwhelming the levees that protect low-lying parts of Auburn, Kent, Renton and Tukwila, the federal agency has warned. "We need to prepare for a long-term possibility that over the next few flood seasons we may experience anywhere from significant to catastrophic flooding, depending on the event," said a Auburn city spokeswoman. Officials from the four cities, the Corps and King County have been telling businesses and residents about the danger and are urging them to buy flood insurance and be prepared to evacuate in the event of a disaster. "We can protect life. We don't know that we can protect property," she said. "We've estimated maybe in the neighborhood of 3,000 people [in Auburn] could be affected in a large-scale event." A larger number of homes and businesses could be hurt in flood-prone parts of Kent, where about 50,000 people work and 22,000 people live, said the mayor. She said the damaged abutment "clearly raises our level of concern" about levees downstream that have not been certified as meeting federal standards. If the substandard Horseshoe Bend Levee were to fail, the Green River Valley could be flooded all the way to Interstate 405 in Renton, possibly severing Highway 167 and two main rail lines.
Source:
http://seattletimes.nwsource.com/html/localnews/2008861523_damdamage15m.html

47. *March 14, Daily Herald* – (Illinois) **Work beginning on new flood control levee.** Local officials from across the region donned hard hats and picked up shovels March 13 during the groundbreaking ceremony for a $26 million levee along the Des Plaines River. About 50 people gathered to listen to various officials talk about the long process of winning approval for construction of Levee 37 in Mount Prospect and Prospect

Heights. The flood control project is expected to prevent the destruction of Mount Prospect and Prospect Heights homes and businesses whenever the river floods during major storms. A main flood wall will be built along the east side of River Road and Milwaukee Avenue, between Euclid Avenue and Palatine Road. It is expected to be completed in about two years. In addition to the levee, three pump stations with 20,000 gallons per minute pumping capacity will be built. About 600 residences and dozens of businesses will be protected, officials said.
Source: http://www.dailyherald.com/story/?id=278954

48. *March 13, Crookston Daily Times* – (Minnesota) **All signs point to high water.** The updated spring flood outlook issued by National Weather Service hydrologists on March 13 includes a 90 percent chance the Red Lake River in Crookston will reach 21.5 feet, a 50 percent chance it will reach 23.5 feet, a 20 percent chance it will reach 26 feet, and a 10 percent chance it will reach 27 feet. In more general terms, the outlook states that there is a 50 percent chance or greater of major flooding in Crookston. After reading through the data, the Crookston emergency manager and the community development director sat down at city hall on Friday to go over the latest survey maps that show the various dike elevations throughout town, in areas where flood control projects are complete, are in progress, and also in areas where the temporary levee system erected more than 40 years ago is still in place.
Source: http://www.crookstontimes.com/news/x1676803004

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure 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

DHS Daily Open Source Infrastructure Report 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