



Homeland Security

Daily Open Source Infrastructure Report for 9 July 2009

Current Nationwide Threat Level

ELEVATED



Significant Risk of Terrorist Attacks

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

Top Stories

- According to DEBKAfile, Western anti-terror agencies have warned that a group of 15-20 al Qaeda terrorists, who were trained in Pakistan and Algeria to hijack and blow up U.S.- and Israel-bound airliners, deployed secretly to at least six European and Middle East countries in early July. (See item [14](#))
- The Washington Post reports that South Korea's intelligence agency suspects that North Korea may have been behind an Internet attack that on Tuesday and Wednesday targeted government Web sites in South Korea and the United States. Web sites operated by Nasdaq, the New York Stock Exchange, and the Washington Post were also attacked. (See item [23](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams Sector](#)

SUSTENANCE AND HEALTH

- [Agriculture and Food](#)
- [Water Sector](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL AND STATE

- [Government Facilities](#)
- [Emergency Services](#)
- [National Monuments and Icons](#)

Energy Sector

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

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

1. *July 8, Platts* – (International) **Shell says investigating latest Nigeria pipeline attack.**
Anglo-Dutch major Shell on July 8 said it was investigating the attack on the company's

Nembe creek trunk line in Nigeria's southern Bayelsa state by armed militants. "We are investigating reports of an attack on SPDC joint venture's Nembe creek pipeline," a Shell spokeswoman told Platts. Nigeria's main militant group MEND, or the Movement for the Emancipation of the Niger Delta, said on July 8 that it sabotaged major oil pipelines operated by Shell and Italy's Eni in southern Bayelsa state. "The plague of sabotage descended heavily on major Shell and Agip crude trunk lines in Bayelsa state at about 2:00 am and 2:30 am [01:00-01:30 GMT] Wednesday," MEND said in an emailed statement. MEND said the Eni Agip pipeline connects to the Brass export terminal and was sabotaged at Nembe creek, while the Shell Nembe creek line was attacked at Asawo village in the southern Bayelsa state. MEND linked the attacks on July 8 to the army's arrest of two militants who approached the military to surrender their arms in line with the government's amnesty offer.

Source:

<http://www.platts.com/Oil/News/8693880.xml?sub=Oil&p=Oil/News&?undefined&undefined>

2. *July 7 Associated Press* – (Pennsylvania; New Jersey) **Overtaken tanker truck closes Pa.-N.J. bridge.** An overturned tanker truck carrying propane has closed a bridge connecting Pennsylvania and New Jersey. The crash happened around 12:15 p.m. on July 7 on the Commodore Barry Bridge, a short distance down the Delaware River from Philadelphia. The bridge links the Pennsylvania city of Chester with Bridgeport, New Jersey. The truck is blocking the westbound lanes, and the eastbound lanes have also been shut down. A spokeswoman for the bridge's operator, the Delaware River Port Authority, says a hazmat team is on the scene to deal with a small diesel fuel leak. The bridge is located about 15 miles southwest of Philadelphia.

Source:

http://www.philly.com/philly/wires/ap/news/state/pennsylvania/20090707_ap_overtaken_tanker_truck_closes_panj_bridge.html

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

Chemical Industry Sector

3. *July 7, KTRE 9 Lufkin* – (Texas) **Major chemical spill leaves hazmat crew cleaning up for hours.** "Around 6:30 this morning, an 18-wheeler lost control and turned over several times," said the Shelby County hazmat chief. When the fire department arrived on scene on July 7 in Lufkin, the driver had already climbed out of the truck, but the toxic chemical the truck was carrying had spilled all over the ground on Highway 59 between Timpson and Tenaha. The chemical is an organic peroxide that the hazmat chief said is shock sensitive. It reacts with soil, auto-ignites, and explodes. He said it is extremely toxic to the human body. They have been working since early Tuesday morning to off-load by hand every five gallon container from the truck, and there are over 400 of them. They expect Highway 59 to remain closed until around 7 or 8 p.m. on July 7, and most of the residents that were asked to evacuate have already been allowed to return home.

Source: <http://www.ktre.com/Global/story.asp?S=10659295&nav=2FH5>

Nuclear Reactors, Materials, and Waste Sector

4. *July 7, Associated Press* – (Connecticut) **Conn. Nuclear plant closed after lightning strike.** The Millstone 2 nuclear reactor in Waterford remains shut down, four days after lightning apparently hit a power line and affected power systems. A spokesman for Dominion, Millstone's owner, says the power station shut down Friday after electricity coming to the power station fluctuated and affected the operation of the turbine. A spokeswoman for the Nuclear Regulatory Commission (NRC) says the plant is stable and did shut down safely. An official with the NRC says there were no radioactive releases associated with the incident or any impact on public health and safety. The NRC's resident inspectors have been examining the situation since Friday and over the holiday weekend.

Source: <http://www.courant.com/news/local/statewire/hc-ap-ct-millstoneshutdownjul07,0,2566812.story>

5. *July 7, Minnesota Public Radio* – (Minnesota) **Safety drills this week at Monticello nuclear plant.** Several hundred emergency responders will descend on Monticello this week for a routine safety drill at Xcel Energy's nuclear power plant that will take place throughout the day Wednesday and Thursday. The drills, which have taken place for more than a dozen years, alternate each year between the Monticello and Prairie Island nuclear facilities. Emergency responders will go through a scenario in real time, to test their ability to take decisive action in an emergency incident, the spokesman said. Terrorist attacks are "the worst-case scenario, and we haven't even come close to anything like that in the state in the past," the spokesman said. Officials with the state's Department of Public Safety, the U.S. Department of Homeland Security, Xcel Energy, the State Patrol, the Department of Agriculture and operators of the nuclear plant will participate in the drill.

Source: http://minnesota.publicradio.org/display/web/2009/07/07/nuclear_drill/

Critical Manufacturing Sector

6. *July 7, WJHL 11 Johnson City* – (Tennessee) **Fire is now out at J.C. scrap metal plant.** A fire that started late Monday night at the OmniSource Corporation is now out. OmniSource is a scrap metal processing plant located in Johnson City. The Johnson City and Jonesborough Fire Departments responded to a heap of scrap metal that caught on fire shortly after 11 p.m. on July 7 causing massive flames. Fire crews say they cleared and turned the scene back over to OmniSource officials just before 6 a.m. Fire officials say that magnesium burning in a pile of scrap cars, miscellaneous appliances and sheet metal made this fire particularly difficult to put out. Fire officials tell us that nobody was injured during the blaze. They have not released a cause for the fire at this time.

Source:

http://www.tricities.com/tri/news/local/article/j.c._scrap_metal_plant_on_fire/28290/

7. *July 7, Associated Press* – (Nevada) **NV gold mine fined \$500,000 for fatality.** Federal regulators have fined Newmont Mining Corp. more than \$500,000 for safety violations they say contributed to the death of a worker at an underground gold mine in Nevada. The Mine Safety and Health Administration also announced on July 7 that four supervisors for the Denver-based mining company have agreed to pay a combined \$60,000 in individual penalties for their role in the accident at the Midas Mine north of Elko in June 2007. The agency said managers “showed a disregard for the miners’ welfare” and acted with “more than ordinary negligence” before the victim fell through a sinkhole while operating a large loader about 200 feet below the entrance of the mine. The violations included failure to provide adequate controls to guard against cave-ins and failure to provide adequate barricades and signs to warn miners about the hidden hazards of sinkholes. In addition, Newmont was cited for impeding MSHA’s investigation of the accident by failing to provide maps and other documents, as well as failing to report the entrapment within the required 15 minutes. The first-line supervisor, two general foremen and the engineer in charge agreed to pay the \$60,000 for their roles in the “flagrant ground control violation,” the agency said. Their names were not immediately released.
Source: <http://www.google.com/hostednews/ap/article/ALeqM5hypFVwYjT260-8uzBAqi54rDh2uwD999T0T00>
8. *July 7, Lahontan Valley News* – (Nevada) **Little damage reported at Kennametal plant fire.** An electrical fire at the Kennametal plant 10 miles north of Fallon resulted in the closure of U.S. Highway 95 for four hours on July 4 as firefighters attempted to determine if any chemicals were involved. The Fallon Churchill volunteer fire chief said the department was notified of the fire at 7:46 p.m., but it was unable to access the location until 10 p.m. until he was notified if chemicals were stored there. One ladder truck and one ambulance were on the scene. He said a 24 x 24 building was completely destroyed, and added he did not know the value of the structure or the equipment that was inside. The Nevada Highway Patrol closed U.S. Highway 95 at Trinity (I-80) and northbound traffic out of Fallon was turned around. The fire was extinguished in 15 minutes once firefighters started fighting it.
Source: <http://www.lahontanvalleynews.com/article/20090707/NEWS/907079998/1055>

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

Defense Industrial Base Sector

9. *July 6, BusinessWeek* – (National) **Under cyberthreat: defense contractors.** The defense industry faces “a near-existential threat from state-sponsored foreign intelligence services” that target sensitive IP, according to a report by the Internet Security Alliance, a nonprofit organization. Northrop Grumman experienced the implications of that threat firsthand recently. According to a Frontline investigation that aired June 23, reporters were able to purchase an unencrypted hard drive of a Northrop Grumman employee in Ghana for \$40. The drive reportedly contained hundreds of documents about government contracts. “It’s gotten to a point where it has a name for itself: the APT or ‘advanced persistent threat,’ meaning that they are well resourced, highly sophisticated, clearly targeting companies or information, and they’re not giving

up in that mission,” said a former FBI agent and foreign counterintelligence expert. “Attribution is probably one of the biggest problems for our nation, both from a defensive and an offensive posture as a country. Obviously we know that the likes of China and Russia have the greatest capabilities, like the U.S., from an espionage perspective. But we are starting to see quite a capability in the organized crime, criminal aspect. Clearly you’re seeing this with a lot of the credit-card or financially motivated crimes that are occurring...Most of the attacks in about the last three to four years have [involved] legitimate credentials. The analogy would be that they had a set of keys to your home and they know the codes to your alarm system at home so they can enter and leave as they please, without leaving a track unless you’re looking for things like entering during an abnormal hour of the day when you’re at work. Obviously, Northrop is a world-class operation when it comes to both offensive attack and exploitation of networks and defense, which is my area of expertise.”

Source:

http://www.businessweek.com/technology/content/jul2009/tc2009076_873512.htm?chan=technology_technology+index+page_top+stories

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

Banking and Finance Sector

10. *July 8, New York Times* – (International) **Swiss vow to block UBS from handing data to U.S.** The Swiss government said on July 8 that it was prepared to seize UBS client data rather than allow the bank to hand it over to the United States to settle a tax case, the New York Times reported. UBS has refused a demand from U.S. authorities that it turn over the names of 52,000 American clients, arguing that to do so would be illegal under Swiss banking secrecy laws and would open it to prosecution at home. The U.S. Justice Department in February sued UBS, saying it suspected the bank of helping wealthy Americans hide billions of dollars in secret offshore accounts. “Switzerland makes it perfectly clear that Swiss law prohibits UBS from complying with a possible order by the court in Miami to hand over the client information,” the Swiss Department of Justice and Police said on July 8 in a statement on its Web site, a day after it made a filing to the same effect in the U.S. District Court in Miami. Therefore, “all the necessary measures should be taken to prevent UBS from handing over the information on the 52,000 account holders demanded in the U.S. civil proceeding,” it added. The Swiss government will issue an order explicitly prohibiting UBS from handing over client information “if circumstances require,” it said. UBS, the largest Swiss bank, is under great pressure to reach an agreement. The bank has already paid \$780 million and turned over the names of more than 250 clients to avoid prosecution on allegations that it defrauded the Internal Revenue Service. Its soured investments, many on American subprime mortgages, have cost it \$53 billion in write-downs, sending it to taxpayers for a bailout. UBS officials were not immediately available for comment.

Source: <http://dealbook.blogs.nytimes.com/2009/07/08/swiss-vow-to-block-ubs-from-handing-data-to-us/>

11. *July 8, Associated Press* – (Georgia) **Suspicious package found at Bank of America branch.** A suspicious package found at a Bank of America branch in Atlanta was found

to contain ammonium chloride. Authorities cleared the bank on Ponce de Leon when the package was found about 11:45 a.m. on July 7. Firefighters wearing hazardous material suits removed the package after bomb squad personnel determined it was not an explosive device. Ammonium chloride is salt-like in its purest form, is sold in blocks at hardware stores and has varied industrial and manufacturing uses. It can induce nausea or vomiting. Authorities said the U.S. Department of Homeland Security is working with bank officials on the investigation.

Source: <http://www.walb.com/Global/story.asp?S=10661037>

12. *July 7, Reuters* – (National) **U.S. SEC charges Provident Royalties in \$485 mln fraud.** Provident Royalties LLC and three founders were charged with securities fraud for allegedly bilking thousands of oil and natural gas investors in a \$485 million Ponzi scheme, the Securities and Exchange Commission said on July 7. In a civil case, the SEC alleges that from about September 2006 until January 2009, Texas-based Provident Royalties raised nearly half a billion dollars from at least 7,700 U.S. investors by promising annual returns of over 18 percent and misrepresenting how the funds would be used. A portion of the proceeds were used for acquisition and development of oil and gas exploration and development activities, but other investor funds were used to pay earlier Provident Royalties investors, the SEC said. “Investors were told that 86 percent of their funds would be placed in oil and gas investments. That representation was false,” the SEC’s complaint said. The SEC said a federal court issued an emergency freeze on assets and appointed a receiver to preserve the assets.

Source:

<http://www.reuters.com/article/governmentFilingsNews/idUSN0732721720090707>

13. *July 7, Wall Street Journal* – (California) **Big banks don’t want California’s IOUs.** A group of the biggest U.S. banks said they would stop accepting California’s IOUs on July 3, adding pressure on the state to close its \$26.3 billion annual budget gap. The development is the latest twist in California’s struggle to deal with the effects of the recession. After state leaders failed to agree on budget solutions last week, California began issuing IOUs, or “individual registered warrants,” to hundreds of thousands of creditors. The state controller said that without IOUs, California would run out of cash by July’s end. But now, if California continues to issue the IOUs, creditors will be forced to hold on to them until they mature on October 2, or find other banks to honor them. When the IOUs mature, holders will be paid back directly by the state at an annual 3.75 percent interest rate. Some banks might also work with creditors to come up with an interim solution, such as extending them a line of credit, said a California Bankers Association spokeswoman. Amid the budget deadlock, Fitch Ratings on July 6 dropped California’s bond rating to BBB, down from A minus, the latest in a series of ratings downgrades for the state. The group of banks included Bank of America Corp., Citigroup Inc., Wells Fargo & Co. and J.P. Morgan Chase & Co., among others. The banks had previously committed to accepting state IOUs as payment. California plans to issue more than \$3 billion of IOUs in July.

Source: <http://online.wsj.com/article/SB124692354575702881.html>

For another story, see item [23](#)

Transportation Sector

14. *July 8, DEBKAFile* – (International) **U.S., German intel: Al Qaeda plots multiple attacks on U.S.-, Israel-bound airliners.** Western anti-terror agencies have warned that a group of 15-20 al Qaeda terrorists, who were trained in Pakistan and Algeria to hijack and blow up airliners, deployed secretly to at least six European and Middle East countries in early July. They are standing ready to carry out multiple terrorist attacks. The terrorists are believed to have landed in Britain, Germany, France, Italy, Turkey and Egypt. The dates to watch, local authorities were warned, were July 4, July 7, the fourth anniversary of the 7/7 attacks on the British transport system in which 52 people died, and July 8-9, when the G8 summit meets in the Italian town of L'Aquila. The U.S. President will fly in from talks with Russian leaders in Moscow. Al Qaeda planners, say the Western sources, know it is extremely hard to break through the massive security cordons protecting summit leaders. They are therefore planning to hijack passenger planes of airlines belonging to the targeted states and blow them up in mid-air. DEBKAFile's counter-terror sources report the first specific red alert on July 4, referred to the possible hijack of Turkish Airways planes taking off from Turkish airports for U.S. destinations or Tel Aviv. According to WTOP 103.5 Washington, D.C., Turkish Airlines flies directly to New York and Chicago.

Source: <http://www.debka.com/headline.php?hid=6169>

See also: <http://www.wtop.com/?nid=778&sid=1711695>

15. *July 8, St. Charles Sun* – (Illinois) **Big safety issues roll into Wayne on CN rails.** It only lasted about two minutes, leaving about six cars idling on Army Trail Road. The Canadian National (CN) freight train quickly rumbles south on the tracks it now owns, a portion of which run through Wayne. The train's short appearance late on the morning of July 2 contrasts with police reports that show at least six instances since February 23 where Canadian National officials were called because either a train or malfunctioning gates stalled traffic for anywhere between 10 minutes to an hour and 19 minutes. Before CN, such a problem would occur once or twice a year. "We obviously have no forewarning of when that's going to happen," a police chief said of the long delays. Each blockage splits the village in half, requiring the small police force to have a squad car on each side and a plan in place for firefighters to respond from either St. Charles, Bartlett or West Chicago, he said. "It's only a matter of time before something happens," said the village president. Since March, trains on the CN line have grown in length, but not significantly in number, on the semicircle of tracks that used to be known as the Elgin, Joliet & Eastern Railway line. CN's ultimate plan aims to ease freight congestion inside that perimeter in areas such as Chicago and several suburbs on its border.

Source:

http://www.suburbanchicagonews.com/stcharlessun/news/1656379,2_1_AU08_WAYN E_S1-090708.article

16. *July 8, Aero-News Network* – (Florida) **Guilty plea in charter jet fraud case.** A former executive with Platinum Jet Management in Fort Lauderdale, Florida, has pleaded guilty

to fraud charges stemming from a 2005 accident in New Jersey. The executive admitted hiring unqualified pilots to fly charters for Platinum. The Associated Press reports one of those pilots was acting as pilot in command of a charter jet that aborted its take off, slamming into a warehouse at Teterboro Airport and injuring 20 passengers along with both pilots and two occupants of a vehicle on the ground, according to the Wall Street Journal. An NTSB investigation showed that the pilot failed to ensure proper weight and balance on the aircraft prior to departure, and that the center of gravity was too far forward, causing it to not rotate at the proper speed. The New Jersey court documents indicate the executive and his co-defendants contracted with unqualified pilots and allowed them to fly Part 135 charters, and then conspired to conceal regulatory violations by falsely logging those flights as private Part 91 flights. Wire fraud occurred when those documents were faxed across state lines. The Journal reports that the executive admitted in court that he dispatched the pilots on that plane knowing they were not qualified to fly it, and that he had done the same thing on other flights, while telling charter brokers Platinum complied with federal laws. Four of his co-defendants are also charged with falsifying weight and balance graphs to make it appear that the aircraft were within COG limits when in fact they were not and again faxing those graphs over state lines.

Source: <http://www.aero-news.net/index.cfm>

17. *July 7, Aviation Herald* – (Maryland) **Southwest B733 at Baltimore on Jul 7th 2009, flock of birds strike.** A Southwest Airlines Boeing 737-300, flight WN-69 from Baltimore, Maryland to Providence, Rhode Island with 126 people on board, struck a flock of birds while taking off Baltimore's runway 28. The airplane was cleared for an immediate landing at runway 33L, where the airplane landed safely about 10 minutes after liftoff. A runway inspection of runway 28 revealed about 40 carcasses of starling sized birds on the ground just clear of intersection of runway 28 and 33L.

Source: <http://avherald.com/h?article=41c540e1&opt=4865>

For more stories, see items [2](#) and [3](#)

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

Postal and Shipping Sector

Nothing to report

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

Agriculture and Food Sector

18. *July 8, New York Times* – (National) **Administration issues new rules on egg safety.** On July 7, the Presidential Administration released a rule to deal with the nation's egg problem and used the moment to promise a sweeping overhaul of the system to ensure the safety of spinach, lettuce, tomatoes, melons, beef and chicken. In a White House ceremony, the Vice President told Congressional leaders and food regulators that the Administration would make safer foods a priority. "There are few responsibilities more

basic or more important for the government,” he said, “than making sure the food our families in America eat is not contaminated and is safe.” The Agriculture Department promised to develop new standards to reduce salmonella levels in chickens and turkeys by the end of the year. The Food and Drug Administration (FDA) promised to advise the food industry by the end of the July on how to prevent contamination of tomatoes, melons, spinach and lettuce. And within three months, the FDA plans to release advice about how farmers, wholesalers and retailers can build systems to trace contaminated foods quickly from shelf to field. But many rules that even industry representatives call essential are years away. “We’ve got to move to mandatory regulatory standards, and this is a step along the way,” said a food specialist who is a senior adviser at the food and drug agency. Consumer advocates and industry representatives said they welcomed the Administration’s commitment to food safety. The vice president of the United Egg Producers said his industry supported the new rule. About 250 major egg producers in the United States account for 99 percent of fresh egg production, he said, and most already abide by the rule. Since the rule applies only to producers with 3,000 or more laying hens, thousands of small producers are exempt.

Source: <http://www.nytimes.com/2009/07/08/health/policy/08eggs.html?ref=us>

19. *July 7, U.S. Food and Drug Administration* – (New York; Pennsylvania) **FDA takes enforcement action against cheese manufacturer.** The U.S. Department of Justice, on behalf of the U.S. Food and Drug Administration (FDA), filed a complaint on July 7 seeking injunctive relief against Peregrina Cheese, Inc., (Peregrina Cheese), of Brooklyn, New York and two of its officers. The company prepares and processes a variety of cheeses, sour cream, flan and gelatin products and distributes them to specialty grocery stores in northeastern Pennsylvania and in the New York City area. The government’s complaint, filed Tuesday in the Eastern District of New York, alleges that the company has an extensive history of operating under insanitary conditions and producing cheese contaminated with *Listeria monocytogenes*. If entered by the court, the injunction would temporarily stop the company and its officers from manufacturing and distributing food until further action is taken by the court. “This company has consistently failed to make corrections to improve the insanitary conditions under which it processes cheese products, despite frequent warnings to do so,” said the FDA’s acting associate commissioner for regulatory affairs. “The FDA will not tolerate food companies that fail to provide adequate safeguards.” “The public must be able to trust that the food in their grocery stores is safe for them to eat,” said the United States Attorney for the eastern district of New York. As alleged in the complaint, on numerous occasions since 2004, FDA investigators found *Listeria monocytogenes* in finished cheese products and inside Peregrina Cheese’s facility. Additionally, routine laboratory testing by New York State Department of Agriculture and Markets (NYSDAM) also found *Listeria* in the company’s products on numerous occasions since 2003. The FDA and NYSDAM inspections also revealed that the company repeatedly violated the current Good Manufacturing Practice (cGMP) requirements for foods. Investigators found filthy conditions, standing water in food processing equipment, workers inappropriately dressed and a dead rodent inside the plant. No illnesses have been reported to date from Peregrina Cheese products.

Source:

For another story, see item [33](#)

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

Water Sector

20. *July 8, Kalamazoo Gazette* – (Michigan) **Ex-Hartford sewage supervisor fined.** The former superintendent of the Hartford wastewater treatment plant has been fined for knowingly discharging E. coli bacteria into the Paw Paw River. The Van Buren County Circuit Court judge last month fined the former superintendent \$2,500 plus \$120 costs for water-resources protection violations on March 27, 2007 and August 6, 2007 in Hartford. A detective sergeant of the Michigan Department of Environmental Quality said that the superintendent had worked both at Hartford and at the plant on the Paw Paw Lake near Coloma in Berrien County. He received similar charges in Berrien. “He pled and has been sentenced...there already,” he said. According to paperwork on file in the Van Buren County Prosecutor’s Office, the former superintendent admitted he made up data. “The investigation revealed that the superintendent of the Paw Paw Lake Wastewater Treatment Plant submitted falsified ‘daily monitoring reports’ for two months,” according to the report, which covered both cases. The man no longer works at either plant, the detective sergeant said.

Source: <http://www.mlive.com/news/kzgazette/index.ssf?/base/news-34/1247064635189860.xml&coll=7>

21. *July 7, Fort Dodge Messenger* – (Iowa) **Study: Humboldt city water supply at risk.** The Humboldt water supply is at risk, along with aquatic life in the Humboldt and Rutland areas, according to a report by the U.S. Army Corps of Engineers. Humboldt residents heard the report’s results July 6 on the West Branch of the Des Moines River in the Humboldt and Rutland area. The meeting, held at the Oxbow Building in Oxbow Park, was attended by about 35 city and county officials and residents. “The purpose of this document is to tell Congress and our higher headquarters in the Army that there is a project here the Army Corps of Engineers should see,” the project manager with the Corps Rock Island District said. The study was authorized by a committee of the U.S. House of Representatives in 2007. The primary problems identified were the continued shallowing of the river and its affect on aquatic wildlife. In addition, the municipal water supply is at risk from flooding because the water supply plant is within the flood plain. Corps representatives have met with Humboldt city officials about the water plant, the project manager said. Possible ways to improve aquatic wildlife include removal of the dam, construction of a rock ramp or bypass channel to allow the passage of fish, construction of grade control structures to stabilize erosion, or rehabilitation of the gates on the Humboldt Dam. To protect the water plant, the study suggests a floodwall, levees, a flood warning system and the creation of or updating of disaster assistance manual.

Source: <http://www.messengernews.net/page/content.detail/id/516682.html?nav=5010>

For another story, see item [33](#)

Public Health and Healthcare Sector

22. *July 7, Las Vegas Review Journal* – (Nevada) **State health officials order clinic to stop performing surgeries.** State public health officials ordered the Las Vegas Clinica de Mujeres medical clinic to shut down Tuesday because it was performing surgeries without a license. Doors to the small clinic in a deteriorating shopping center were locked late Tuesday afternoon, but there was no sign outside indicating the facility was closed. A spokesman for the Nevada State Health Division's Bureau of Health Care Quality and Compliance said the complaint about the clinic was not made by a patient, but by someone with knowledge about its operation. "No one who complained had a bad outcome," he said. "But there was a gross breakdown in infection control practices." He said that breakdown included breaches in providing sterile packaging and not having a manual or policy for a machine used to sterilize equipment.

Source: http://www.lvrj.com/news/breaking_news/50176272.html

Government Facilities Sector

23. *July 8, Washington Post* – (International) **North Korean agency suspected in cyber-attack.** South Korea's intelligence agency suspects that North Korea may have been behind an Internet attack that on Tuesday and Wednesday targeted government Web sites in South Korea and the United States, lawmakers in Seoul told news agencies. Twenty-six Web sites in the two countries, including the office of South Korea's president and the defense ministry, were targeted, the South Korean National Intelligence Service said in a statement. In the United States, the attack targeted Web sites operated by major government agencies, including the departments of Homeland Security and Defense, the Federal Aviation Administration and the Federal Trade Commission, according to several computer security researchers. "The attacks appear to have been elaborately prepared and executed at the level of a group or a state," the agency said. Eleven Web sites in the United States had problems similar to those that occurred in South Korea, the Korean Information Security Agency said. Some members of the intelligence committee in the National Assembly were told by intelligence officials that North Korea or its sympathizers were prime suspects in the attacks, according to Yonhap, the South Korean news agency, which cited unnamed legislators. The attacks were described as "distributed denial of service," an operation that hacks into personal computers and commands them to overwhelm certain Web sites with a blizzard of data. U.S. government officials declined Tuesday night to confirm the agencies affected by the attack. A Department of Homeland Security spokeswoman said that the agency was aware of ongoing attacks and that the government's Computer Emergency Response Team had issued guidance to public and private sector Web sites to stem the attacks. In addition to sites run by government agencies, several commercial Web sites were also attacked, including those operated by Nasdaq, the New York Stock Exchange, and the Washington Post.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2009/07/08/AR2009070800066.html?nav=hcmodule>

24. *July 7, Associated Press* – (National) **Report: Probe found weaknesses in federal security.** Government investigators smuggled bomb-making materials into federal buildings past the police agency charged with protecting those buildings and found numerous other gaps in security, according to a congressional report. The Government Accountability Office (GAO) said investigators carried bomb-making materials past security at 10 federal buildings. Security at these buildings and a total of about 9,000 federal buildings around the country is provided by the Federal Protective Service, a target of the probe. Once GAO investigators got the materials in the buildings, the report said, they constructed explosive devices and carried them around inside. For security reasons, the GAO report did not give the location of the buildings. The report was made available to the Associated Press in advance of a hearing scheduled Wednesday of the Senate Homeland Security and Governmental Affairs Committee. “The findings of covert security tests conducted by GAO investigators are stunning and completely unacceptable. In post-9/11 America, I cannot fathom how security breaches of this magnitude were allowed to occur,” said a Senator from Maine, the top Republican on the committee. “These security lapses and others show a disturbing pattern by the Federal Protective Service of poor training, lapsed documentation, lax management, inconsistent enforcement of security standards and little rigor.”

Source: <http://www.google.com/hostednews/ap/article/ALeqM5gMYn-01qNRs0d3PzqxFQE7rdH6cQD99A0IT00>

See also: http://voices.washingtonpost.com/federal-eye/2009/07/gao_finds_major_security_flaws.html?hpid=topnews

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

Emergency Services Sector

25. *July 8, WAFB 9 Baton Rouge* – (Louisiana) **Governor Jindal signs emergency shelter bill.** Louisiana’s governor signed a bill into law that will increase Louisiana’s in-state emergency shelter capacity. The new law will allow facilities owned or leased by the state or local governments to be used as shelters during emergency evacuations. The law works to increase shelter space by allowing public facilities owned or leased by the state or local governments, such as schools and postsecondary education facilities, which are suitable for use as public evacuation shelters to be made available at the request of the Governor’s Office of Homeland Security and Emergency Preparedness during an emergency. In addition, \$7.5 million in surplus funds was included in House Bill 2 to support eligible state buildings that need retrofitting and renovations to allow for their use as emergency shelter space under this new law.

Source: <http://www.wafb.com/Global/story.asp?S=10659199>

26. *July 7, KTIV 4 Honolulu* – (Hawaii) **Woman sentenced for stealing ambulance.** A judge sentenced a 23-year-old woman who hijacked an ambulance to nine months in prison on Tuesday. Paramedics were tending to a patient in Kakaako in March when the woman jumped in the ambulance, claimed she had a gun and started driving. The

woman faced a maximum of 15 years in prison after pleading guilty to all charges including second-degree robbery and second-degree assault.

Source: <http://www.kitv.com/mostpopular/19983077/detail.html>

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

Information Technology

27. *July 8, Spamfighter News* – (International) **Trend Micro discovers new ransomware ‘WORM_RANSOM.FD.’** According to Trend Micro security researchers, they have detected a new ransomware that proliferates through an e-mail on the internet. Trend Micro have called the malware WORM_RANSOM.FD that seems as a mass mailing computer worm, but a detailed analysis of it has revealed that it contains a deadly payload. It has been discovered that WORM_RANSOM.FD downloads from remote websites when visitors access those sites or it may download secretly by other malware on the targeted system. While the deadly payload does not affect some files with extensions such as .dry, .rwg, .vxd, .dll, .inl and .exe, the malware is capable of encrypting all files stored in the targeted computers using Blowfish algorithm. Hence, the malware makes the files useless. Moreover, the worm makes a registry entry (ies) that allows it to do automatic execution whenever the system startup. Interestingly, the new ransomware WORM_RANSOM.FD does not follow the function of a typical ransomware which demands money for restoring encrypted files. Instead it gives a user three options to choose from to restore the affected files.
Source: http://www.spamfighter.com/News-12686-Trend-Micro-Discovers-New-Ransomware-WORM_RANSOMFD.htm
28. *July 7, IDG News Service* – (International) **Software developer pleads guilty to spam charge.** A Virginia software developer has pleaded guilty to charges related to creating and marketing software designed to send bulk commercial e-mail messages, in violation of the U.S. CAN-SPAM Act, the U.S. Department of Justice said. The guilty party, 49, of Centreville, Virginia, pleaded guilty on July 7 to aiding and abetting violations of the CAN-SPAM Act committed by two spam kingpins, both of West Bloomfield, Michigan, and other spammers, the DOJ said. Under the terms of his plea agreement, the guilty party faces up to six years in prison, a fine of \$3,000 and the forfeiture of \$50,100 in proceeds for the sale of his software. He pleaded guilty in U.S. District Court for the Eastern District of Michigan. From January 2004 to September 2005, the guilty party and his company, Lightspeed Marketing, developed and sold customized software products that allowed users to send large volumes of spam e-mail at high speeds and disguise the true origin of the e-mails from recipients in order to evade antispam filters, blacklisting and other spam-blocking techniques, the DOJ said. The guilty party, in his plea agreement, acknowledged that he designed the Nexus software package to enable users to insert false information into the headers of the spam e-mails it sent, the DOJ said. The accused designed Proxy Scanner to enable users to make use of third-party proxy computers to relay or retransmit spam e-mails and disguise their true origin.
Source: http://www.pcworld.com/businesscenter/article/168007/software_developer_pleads_guilty_to_spam_charge.html

For another story, see item [23](#)

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

29. *July 7, Ventura County Star* – (California) **Construction mishap wipes out phone, Internet, ATM service.** A damaged fiber-optic cable caused a massive telecommunications failure on July 6 in Ventura County, slowing commerce and shutting down 911 emergency systems. The problem lingered through most of the day in Oxnard, Camarillo, Newbury Park, Santa Paula, Port Hueneme and Malibu, said a spokesman for Verizon Communications. Police departments in Oxnard and Santa Paula as well as the Ventura County Fire Department could not receive emergency 911 calls for most of the day. The outage, reported about 10 a.m., slowed or shut down phone lines, cell phone towers, Internet service and credit card and ATM machines, the spokesman said. By 5:30 p.m., just a few areas in Oxnard were still without service. Oxnard police reported that 911 service was restored in the city about 9 p.m. The outage was caused by construction damage to a “general service” fiber-optic cable in Camarillo, which also affected TV and radio stations. Video service for customers who have Verizon’s FiOS service was also affected. Verizon located the broken cable on July 6 at a county road-widening project in Camarillo at Lewis and Dawson roads. Construction workers damaged about 1,000 feet of the several-inches-thick cable, the spokesman said. Source: <http://www.venturacountystar.com/news/2009/jul/07/construction-mishap-wipes-out-phone-internet-atm/>
30. *July 7, IDG News Service* – (National) **Cisco to put routers in space.** At its user conference in San Francisco last week, Cisco Systems boasted about the 30 new businesses it is developing. One is scheduled to launch by the end of this year. The company that pioneered the Internet router is about to enter a new frontier, sending one into geostationary orbit on a satellite. It is the first big step in a U.S. Defense Department-led initiative, called Internet Routers In Space (IRIS), that could eventually make it easier and less expensive to get high-speed Internet access where wires and cables do not reach. Satellites carry Internet data and connect to the Internet through base stations on the ground, but they are really a separate network, said the general manager of IRIS at Cisco. An Earth station beams a signal up to the satellite at a certain frequency, and the craft bounces it back down to another, predefined Earth station. Users, such as service providers and government agencies, have to lease that frequency and sit on it whether they are using it or not. Satellite links represent discrete point-to-point connections in an Internet that is designed to route packets around the world on

any peering network and any kind of physical link. That is because there are no routers in space, according to the general manager. If communications satellites had routers, they could take in IP (Internet Protocol) packets and send them to a variety of places, via different Earth stations or other satellites, forging new links whenever needed. Rather than having to pick a particular link and lease it, users could just pay for an Internet service that uses satellites as part of its physical backbone.

Source:

http://www.businessweek.com/technology/content/jul2009/tc2009077_737978.htm

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

Commercial Facilities Sector

31. *July 7, WALB 10 Albany* – (Georgia) **15 cameras now watching downtown Albany.** Fifteen downtown Albany, Georgia, cameras got their first test with the city's Fourth of July celebration and are now watching the area day and night. The cameras are spread out from the Thronateeska Heritage Center to the Civic Center and from the River to Jackson Street. They are monitored from the 911 Center, but eventually the web based program can be monitored from individual computers. During Saturday's Fourth of July celebration an APD officer was stationed in the 911 center to monitor the cameras, looking for potential trouble. Overnight the cameras can alert dispatchers to movement in specific areas.

Source: <http://www.walb.com/Global/story.asp?S=10658040>

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

National Monuments & Icons Sector

Nothing to report

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

Dams Sector

32. *July 7, Press of Atlantic City* – (New Jersey) **Millville police say kayaker found WWII-era ordnance.** A kayaker out for a late afternoon paddle in Millville discovered a piece of World War II-era ammunition along the shore of the Maurice River, police said. The unexploded ordnance, which police said resembled a large bullet without its shell casing, prompted a call first to the Millville Police and then to Atlantic City's bomb squad for its eventual removal. A Millville Police lieutenant said the ordnance was reported by the kayaker at 5:46 p.m. When police arrived on the scene, they identified the ordnance, which he estimated to be about 8 inches long and 3 inches in diameter, and called Atlantic City for assistance. The area, less than 100 yards from the Union Lake dam, was cordoned off, although two adjacent youth baseball fields and a playground were not evacuated. He said the bomb squad was called in to handle the ordnance, but it did not pose a risk to anyone nearby. Millville police watched as two officers from the bomb squad worked at recovering the ordnance. After it was deemed

stable, the ordnance was removed from the water and X-rayed. He said it will be taken to Atlantic City and likely destroyed. If it was unstable, he said, it would have been detonated on the spot. He could not confirm the age of the ordnance, but did say it resembled other pieces of World War II-era ammunition that have been recovered in Millville.

Source: http://www.pressofatlanticcity.com/news/press/cumberland/article_944e34ad-03dc-5d98-85d7-f2d38c2050ad.html

33. *July 6, Daily City Gate* – (Iowa) **Check point raises concerns.** Officials from the City of Keokuk, Iowa, and Roquette America, Inc. are expected to discuss a security gate issue raised at last week's Keokuk city council workshop. The gate, which is not operative yet, is located behind the flood gate that protects the city's wastewater treatment plant as well as the Roquette plant along the Mississippi riverfront. The plant engineering director of Roquette told the council "this will be a check point more than an actual security gate." Anyone wanting to come inside the check point would have to identify themselves and provide a driver's license number, including anglers who often park near the wastewater treatment plant and fish on the nearby levee. A council member suggested that Roquette erect a fence around its plant instead. After Roquette hired a security firm to make a recommendation, Roquette came up with the idea of a security gate or check point that is manned 24/7, according to the director. Roquette then talked to the Burlington Northern Santa Fe Railroad, which was satisfied with the plan, he said.

Source:

<http://www.dailygate.com/articles/2009/07/06/news/doc4a5246bd865fa835900490.txt>

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

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 NICCRports@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

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.