Top Stories

- Reuters reports that U.S. authorities have charged 1,215 people in hundreds of mortgage fraud cases that resulted in estimated losses of $2.3 billion, top presidential administration officials said June 17, unveiling a crackdown after the housing market collapse. (See item 16)

- A nationwide alert has been issued for 17 members of the Afghan military who have gone AWOL from an Air Force base in Texas where foreign military officers who are training to become pilots are taught English, according to Fox News. The lookout bulletin states that Afghan officers and enlisted men have security badges that give them access to secure U.S. defense installations. (See item 42)

Fast Jump Menu

PRODUCTION INDUSTRIES
- Energy
- Chemical
- Nuclear Reactors, Materials and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH
- Agriculture and Food
- Water
- Public Health and Healthcare

SERVICE INDUSTRIES
- Banking and Finance
- Transportation
- Postal and Shipping
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE
- Government Facilities
- Emergency Services
- National Monuments and Icons

Energy Sector

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

1. June 18, WFOR 4 Miami – (Florida) Miami residents scramble after gas explosion. Residents were told to scramble out of their homes for fear a propane fire
would spread through a Miami neighborhood Thursday night. An apparent accident with a delivery truck at a gas depot sparked an explosion that shut down streets while the fire burned for hours. City of Miami fire officials said a delivery truck operator was filling up when he forgot to disconnect the pump hose from his truck. As a result the line caught fire. His tanker has 12,000 gallons of propane gas inside. Flames could be seen shooting in the air from the area of 3250 NW North River Drive, where the Flori Gas company is located, concerning businesses and neighbors in the area. Police shut down streets in the area for safety reasons. Firefighters were seen yelling at residents to get out of their homes and out of the area for fear the fire might spread. No injuries have been reported so far, but several fire rescue units are on scene. While the fire continues to burn, firefighters wait for the tank to cool off and fight the fire more aggressively.


2. *June 17, USA Today* – (National) **BP’s next challenge: disposal of tainted sludge.** Oil giant BP is facing a new challenge in disposing of the millions of gallons of potentially toxic oil sludge its crews are collecting from the Gulf of Mexico, according to industry experts and veterans of past spills. Crews so far have skimmed and sucked up 21.1 million gallons of oil mixed with water, according to the Deepwater Horizon Unified Command. Because the out-of-control well may continue spewing for months, that total almost certainly will surge. BP’s plan for handling the gooey mess, written in conjunction with the Coast Guard, the Environmental Protection Agency and Louisiana officials, calls for reclaiming or recycling as much as possible. Some experts said that approach is the best option for the environment, but it has not worked in previous spills. It is not profitable to refine sludge that has mixed with water and seagoing debris because it can actually ruin refineries, they said. “It has no longer got any economic value. It has to be disposed of as garbage,” said a former Navy officer who helped oversee numerous oil-spill cleanups, including the 1989 Exxon Valdez in Alaska. “The stuff that got recovered from the Exxon Valdez was just a nightmare.”


3. *June 17, Bay City News* – (California) **Fire crews called to Valero refinery for second time.** Fire crews Thursday night were called to the Valero refinery in Benicia, California for the second time in the same day for an incident in which steam mixed with petroleum coke, a byproduct of the refining process, sending a plume of smoke into the air. “There was a big column of brownish smoke coming up ... probably 200 feet in the air,” the Benicia fire marshal said. The incident was reported at 8:51 p.m. One worker was being medically evaluated at the scene. A similar incident occurred at the refinery Thursday morning, slightly injuring several employees. None had to be hospitalized and they all returned to work afterward, a refinery spokeswoman said. The incident was reported at 10:10 a.m. There was a leak in a unit involving a byproduct that is eventually made into charcoal briquets. Employees were asked to shelter in place until the all-clear signal was sounded at about 11:45 a.m. The morning leak did not have any adverse impacts on the surrounding community. The fire marshal said it is not yet clear whether the accidents are related, but said it does not appear they happened in the same area of the refinery.
For another story, see item 6

Chemical Industry Sector

4. June 18, WSAZ 3 Huntington – (West Virginia) DuPont completes investigations into chemical leaks. DuPont has completed its investigations into a series of chemical leaks that took place at its plant in Belle, West Virginia. The investigation is a result of three leaks that happened in January 2010, including one that went unnoticed for almost a week. After the leaks, company leaders put the plant on a temporary safety stand-down. DuPont has submitted its investigation report to the Environmental Protection Agency (EPA) and the other state and federal agencies involved. According to the investigation, the worker had entered the phosgene building to take a reading when one of the hoses failed, causing him to be exposed to the chemical. The investigation also found that the hose failed because of the length of time the hose was in service, physical corrosion concealed by the manufacturer’s label, and pressure buildup in the line. The company also submitted investigation reports on other incidents that occurred during the weekend of January 22, including: the release of approximately 2,000 lbs of methyl chloride due to a failed rupture disk in the 3455 Intermediates Unit; and the release of approximately 22 lbs of 20 percent Oleum due to leaks in a sampling line in the Spent Acid Recovery (SAR) Unit. Company officials said DuPont has made a number of improvements to its procedures and emergency response to prevent similar incidents in the future. At this time, the phosgene-process unit is the only unit that remains under the safety stand-down. Company officials said the other units were restarted once the incident investigations were completed and determined that they could operate safely. State and federal agencies, including the Chemical Safety Board, the Occupational Safety and Health Administration, and the EPA, are still conducting their own investigations.

Source: http://www.wsaz.com/charleston/headlines/96579484.html

5. June 18, Greenville News – (South Carolina) Last of Liberty’s derailed tanker cars cleared of hazardous materials. As remaining hazardous materials were emptied from tankers Thursday, there was no word yet on the cause of the 24-car derailment and chemical spill that resulted in the evacuation of 436 Liberty, South Carolina-area homes. It could be weeks or a couple of months before a cause of the June 10 derailment near Farmers Hill Road and South Norman Street is determined, said a Norfolk Southern spokesman. Transfer of the last of the hazardous materials — two tankers of ethylene glycol and two tankers of isopropyl alcohol — into other tank cars was complete Thursday, said the Pickens County Emergency Management director. Workers also loaded non-hazardous materials into trucks to be moved from the scene, and more contaminated soil was removed from the site. State Department of Health and Environmental Control (DHEC) staffers walked five or 10 miles of an unnamed stream.
near the derailment, and found no evidence of any problem. Barriers erected at the site prevented contaminated runoff from washing into the stream during recent thunderstorms. A contractor employed by Norfolk Southern is taking water samples upstream and downstream of the derailment site, and DHEC is looking for any residential wells in the immediate area and may do well studies to be sure there is no groundwater contamination. It appears that most, and possibly all homes in the immediate area are on public water lines. DHEC is requiring Norfolk Southern to develop a long-term groundwater sampling plan, which is routine in this type of situation and not an indicator of any problem.

6. June 17, Global Security Newswire – (National) **Stronger antiterror regulations urged for U.S. chemical sites.** Chemical-security advocates are calling for Congress to pass stronger regulations on the types of chemicals used at U.S. facilities, pointing to the BP oil spill in the Gulf of Mexico as evidence of private companies’ lack of preparation for a possible terrorist attack, Greenwire reported June 16. “The BP spill in the Gulf shows undeniably that worst-case scenarios can and do happen, and they can and do overwhelm any emergency response capacity,” said a Center for American Progress consultant on high-risk chemical sites. “Oil in the water is really bad. Chemicals in a big city could be even worse.” One chemical used by the oil industry to aid in the conversion of crude oil into gasoline is hydrofluoric acid. The acid is extremely poisonous for humans and has been judged by the U.S. Centers for Disease Control and Prevention to be a potential, chemical terrorism threat. The hydrofluoric acid housed at BP’s Texas City site could endanger up to 550,000 residents if it were to be released, the oil firm acknowledged recently to the U.S. government.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20100617_6935.php

7. June 17, Danville News and WSLS 10 Roanoke – (Virginia) **Tanker wreck kills driver, leaks chemicals.** A North Carolina man driving a tanker truck was killed early Wednesday morning after his truck ran off U.S. 29 in Pittsylvania County, Virginia, and overturned, Virginia State Police said. The refrigerated truck, owned by Air Products and carrying liquid oxygen, was traveling north on U.S. 29 near Carter Lodge Road in Blairs, Virginia shortly after 4 a.m. when the vehicle ran off the road and overturned onto the passenger side, according to a news release. The truck slid approximately 100 yards before resting on its side in the northbound lanes, leaking the liquid oxygen into the median. State police are investigating the wreck, but an officer said the cause was likely driver fatigue, based on tire tracks on the road and grass. Company representatives were on scene helping hazardous-materials and emergency crews assess the situation and whether they needed to transfer the tank’s contents to another tank before towing the truck — but the officer said they ultimately determined that all of the liquid oxygen had already leaked out. The Danville Fire Department, Pittsylvania County Emergency Services, and the Virginia Department of Emergency Management worked throughout the day to clean up the spill and clear the highway of the truck. They also brought in an independent contractor to clean up the median to address Environmental Protection Agency regulations. The highway was completely
Nuclear Reactors, Materials and Waste Sector

8. *June 18, Burlington Free Press* – (Vermont) **NRC: Entergy did not mislead federal panel.** The federal Nuclear Regulatory Commission (NRC) has determined that Entergy Corp. did not provide it with misleading information about the Vermont Yankee nuclear power plant, as the company has acknowledged doing to state officials. Entergy Corp. disciplined several top-level employees for information provided to the state that suggested the Vernon plant did not have underground pipes carrying radioactive material. The pipes came to the forefront in January when Vermont Yankee disclosed they were leaking tritium. In a letter released Thursday afternoon, the NRC regional administrator told Entergy that its investigation had found no similar deception in documents and testimony provided to the commission.


9. *June 18, Michigan Messenger* – (Michigan) **Federal regulators agree to look into more problems with proposed Fermi 3 reactor.** The federal regulators that are considering granting a license for DTE Energy’s proposed Fermi 3 nuclear reactor have agreed to investigate quality assurance violations associated with plans for the new reactor in Newport City, Michigan. Last fall the Nuclear Regulatory Commission (NRC) issued a notice of violation to DTE for failing to have a plan to ensure that work done by contractors met standards. According to the NRC, quality assurance (QA) comprises all planned and systematic actions that are necessary to provide adequate confidence that a structure, system, or component will perform satisfactorily in service. Attributes of a QA program include procedures, recordkeeping, inspections, corrective actions, and audits. In a June 15 ruling, the NRC’s Atomic Safety and Licensing board responded to a petition by a coalition of environmental groups by agreeing to hold a formal hearing on the issue of QA violations. “Quality assurance requires high-grade components and building practices, and is essential for ensuring the safety of this potentially catastrophic electricity source,” the environmental coalition’s attorney said in a statement. “Indifference to quality assurance has led to such catastrophes as the Gulf of Mexico oil disaster, space shuttles and airplanes crashing to the ground, and has already played into nuclear near-misses, as at Davis-Besse, Three Mile Island, and Fermi 1.”

10. *June 18, Brattleboro Reformer* – (National) **Task force: NRC response to tritium leaks appropriate.** A report issued by a Nuclear Regulatory Commission task force concluded the NRC has responded appropriately to the radioactive contamination of groundwater and soil at the nation’s nuclear power plants. “The NRC is meeting its mission of protecting public health, safety, and the environment ...” stated the Groundwater Task Force. The task force was made up of a number of NRC staffers, which issued its report on June 11. It conducted several months of evaluations of the agency’s past, current and planned actions regarding radioactive contamination of groundwater and soil. The task force was established in part in response to a leak of tritiated water discovered at Vermont Yankee nuclear power plant in Vernon in January.


11. *June 17, Palm Springs Desert Sun* – (California) **Third nuclear reactor cap coming through valley.** The third and final gigantic lid for a nuclear reactor is scheduled to make its way through the Coachella Valley in California early next week. The 150-ton lid bound for the Palo Verde nuclear plant near Phoenix began its 10-day trek from the Port of Long Beach Tuesday night, a Bigge Crane and Rigging Co. spokesman said. The load, which is being escorted by the California Highway Patrol, is expected to arrive in the Coachella Valley between Tuesday and Thursday of next week. Because of a sign that will interfere with the transport, the vehicle, which can only go about 5 mph, will cross over from eastbound to westbound lanes and exit the interstate on the Highway 111 on-ramp.

Source: [http://www.mydesert.com/article/20100617/NEWS01/6170303/Third+nuclear+reactor+cap+coming+through+valley](http://www.mydesert.com/article/20100617/NEWS01/6170303/Third+nuclear+reactor+cap+coming+through+valley)

12. *June 17, WSET 13 Roanoke* – (Virginia) **B & W fined $32,500 for chemical spill violation.** A Lynchburg, Virginia company will have to pay a penalty after a workplace accident two years ago. The Nuclear Regulatory Commission has ordered B&W Nuclear Operations Group to pay $32,500 for its failure to have adequate instructions for workers on how to neutralize acid spills. The violation came after an event in April 2008 when a process operator ended up having an eye injury that required medical attention. B&W has 20 days to either pay or request a hearing.


[Return to top]

**Critical Manufacturing Sector**

13. *June 17, Omaha World-Herald* – (Nebraska) **The calm after the storm.** As the Blackhawk helicopter carrying the Nebraska governor banked left for a better view of the flood-swollen Elkhorn River, two things came into clear focus Wednesday: Norfolk will take an economic hit; and with forecasts saying up to 2.5 inches more rain is possible the June 18 weekend, the state’s flooding concerns are far from over. An industrial park on Norfolk’s south end that provides 1,100 jobs was under water, and
the only railroad access was lost when a bridge collapsed into the turbulent river. One of three railroad workers on the bridge at the time remained missing Wednesday. “This is a real mess,” the governor said as the helicopter swooped low for a closer look at the floodwaters inundating the Nucor and Vulcraft steel plants and the Affiliated Foods Midwest distribution center. He said the largest area of damage had occurred around Norfolk. There are two bridges down and 75 miles of road closed or washed out. U.S. Highway 81 was closed to traffic on Norfolk’s south side as floodwaters flowed across the four-lane roadway through TaHaZouka Park.
Source: http://www.omaha.com/article/20100616/NEWS01/706179929

Defense Industrial Base Sector

14. June 17, Associated Press – (Maryland) Md. man charged in plot to steal copper. A federal grand jury has indicted an Annapolis, Maryland man on charges of theft in an alleged plot to steal copper cables worth more than $300,000. The indictment against the 54-year-old man was returned June 15. He was arrested June 17. According to the five-count indictment, he worked at AAI Corp. The federal government bought copper cables and other wire and stored the equipment at AAI. The indictment alleges that he took cables stored at AAI and sold them to a recycling center for cash.
Source: http://wtop.com/?nid=25&sid=1983319

For another story, see item 46

Banking and Finance Sector

15. June 18, USA TODAY – (National) Microsoft opens center for reports of stolen identities, data. In a major step to slow cybercrime, Microsoft June 17 launched a coalition that will serve as a clearinghouse for reports about caches of stolen data stashed all across the Internet. Malicious programs crafted to swipe financial and personal data have come to saturate the Internet — so much so that security researchers routinely ferret out computer servers used by cybercrooks to hoard stolen data. Until now, there was no specific process for reporting such discoveries. The Internet Fraud Alert center — spearheaded by Microsoft, and managed by the National Cyber-Forensics & Training Alliance (NCFTA) — will serve as a reporting hub. Stolen payment-card numbers and online banking-account log-ons will be routed to the issuing banks. The institutions will then decide whether to alert customers, suspend the accounts or pursue legal remedies. Stolen Social Security numbers, birth dates and other personal data will be archived offline by the NCFTA and made available, as needed, to law enforcement. “This fills a big gap in the arsenal of weapons we need to fight online fraud,” said Microsoft’s deputy general counsel. The stakes are high. Phishing scams, just one method of cyberthievery, revolve around tricking Web users into divulging sensitive data. Last year, phishing gangs duped 1 million U.S.
households into losses of $650 million, according to Anti-Phishing Working Group, a consortium of banks, retailers, Internet host providers, tech-security companies, and law enforcement agencies.

16. June 17, Reuters – (International) **Authorities reveal mortgage fraud crackdown, 485 arrests.** U.S. authorities have charged 1,215 people in hundreds of mortgage fraud cases that resulted in estimated losses of $2.3 billion, top presidential administration officials said June 17, unveiling a crackdown after the housing market collapse. The administration has been under pressure to root out mortgage fraud and improve oversight of the housing market after the housing bubble touched off a global economic slide, and led to a cascade of home foreclosures in the United States. Over the last three-and-a-half months, authorities have made 485 arrests in the fraud cases, obtained 336 individual convictions and recovered more than $147 million, the Justice Department said. The announcement comes a day after U.S. prosecutors unveiled charges against the former head of a now-defunct mortgage lender for an alleged fraud scheme that led to multibillion-dollar losses.
Source: http://www.reuters.com/article/idUSTRE65F3E620100617?type=domesticNews

17. June 17, WBBM 780 Chicago – (Illinois) **Serbian national arrested in ATM skimming plot.** A Serbian national living in north suburban Niles, Illinois was arrested June 18 for allegedly trying to buy a device commonly used for ATM skimming. The 59-year-old suspect, whose last known address was on the 8000 block of West Foster Lane, was arrested by FBI special agents at his home, according to an FBI release. He was charged in a criminal complaint filed last week in U.S. district court with one count of attempting to obtain device-making equipment with intent to defraud, which is a felony offense. Beginning in July 2008, the suspect began negotiating to purchase a device commonly used to skim account information from users of ATM machines, the complaint alleges. But unbeknownst to the suspect, the person he was negotiating with was working with the FBI. During the investigation, he allegedly made frequent mentions of the device, which would be used to capture account info and PINs from unsuspecting ATM users. He would then use that information to steal funds from accounts, the release said.

18. June 17, The Montclair Times – (New Jersey; New York) **Feds expose $45M Ponzi scheme.** A Montclair, New Jersey woman surrendered to the FBI June 17 on charges of running a $45-million real estate investment Ponzi scheme, the U.S. Attorney’s office in Manhattan announced. The 58-year-old suspect allegedly bilked more than 20 investors in New York and New Jersey of tens of millions of dollars, allegedly telling her victims she was using their money to buy and renovate homes and sell them for high returns, prosecutors said. However, authorities said, she allegedly used the money to repay previous investors in the pattern of a classic Ponzi scheme, according to the
complaint unsealed June 17 in Manhattan federal court. The suspect is charged with conspiracy to commit wire fraud and wire fraud, authorities said. If convicted, she could face a maximum sentence of 20 years in prison for each of the conspiracy and wire fraud counts.

19. June 17, Krebs on Security – (International) **Sophisticated ATM skimmer transmits stolen data via text message.** Operating and planting an ATM skimmer — cleverly disguised technology that thieves attach to cash machines to intercept credit- and debit-card data — can be a risky venture, because the crooks have to return to the scene of the crime to retrieve their skimmers along with the purloined data. Increasingly, however, criminals are using ATM skimmers that eliminate much of that risk by relaying the information via text message. One particular craftsman, designs the fraud devices made-to-order, even requesting photos of the customer’s targeted ATMs before embarking on a sale. Just as virus writers target Windows because it is the dominant operating system on the planet, skimmer makers center their designs around one or two ATM models that are broadly deployed around the globe. Among the most popular is the NCR 5886. This skimmer sells for between $7,000 and $8,000, and includes two main components: The card-skimmer device that fits over the card acceptance slot and records the data that is stored on the back of any ATM cards inserted into the device; and a metal plate with a fake PIN pad that is designed to sit directly on top of the real PIN pad and capture the victim’s personal identification number (PIN) while simultaneously passing it on to the real PIN pad underneath. Not all skimmers are so pricey: Many are prefabricated, relatively simple devices that fraudsters attach to an ATM and then collect at some later point to retrieve the stolen data.

20. June 16, Arizona Republic – (Arizona) **Goodyear man accused in ‘Hot Head Bandit’ bank robberies.** A man suspected of robbing several Phoenix-area banks previously has been convicted of armed robbery and served time in prison. The 55-year-old suspect, who lives in an unincorporated area near Goodyear, Arizona was arrested June 7 by a Peoria, Arizona police detective who noticed his truck matched the description of a pickup used during a bank robbery in Chandler in April, according to an FBI media release. A criminal complaint filed in U.S. district court June 8 charges the suspect with three counts each of armed bank robbery and brandishing a firearm during a crime of violence, federal court records show. The complaint links the man to three robberies in January and April. Investigators believe the suspect is the “Hot Head Bandit,” who has robbed several banks in the West Valley since August, including ones in Goodyear, Peoria, Litchfield Park and Phoenix. The nickname came from a baseball cap with flames on the bill that he wore during two of the robberies.
21. *June 16, WBAY 2 Green Bay* – (Wisconsin) **Police, credit union warn of phone scam resurfacing.** Menasha, Wisconsin police and Lakeview Credit Union are issuing warnings about a phone scam. Lakeview said numerous automated calls are going out, telling people their credit or debit card has been compromised. Listeners are then asked to enter their credit card number and its expiration date. The credit union said anyone who entered a card number should consider it stolen and request a new card. Police and the credit union said people are receiving these calls at all hours both at home and on cell phones, even if they are on the Do Not Call list. Police remind people that financial institutions do not make unsolicited calls to request information which they already have on file.


22. *June 16, Victoria Advocate* – (National) **Security breach pushes First Victoria to block signature-based transactions on debit cards.** First Victoria bank in Texas placed blocks on its MasterCard debit cards after a small amount of card numbers were compromised by a third-party source. The bank suspects the issue has to do with a merchant somewhere in the southwestern United States, said the senior vice president and bank services manager for First Victoria. The security breach also affects other banks throughout the Southwest. “This is not unique to First Victoria,” he said. “It’s a problem affecting many financial institutions.” The issue began about May 24 for First Victoria and, since then, the bank has made various changes to protect customers’ information. Currently, the bank has blocked signature-based transactions from a variety of stores, including department stores, grocery stores, drug stores, convenience stores and more. Such transactions are also blocked in a number of countries, as well as the state of Michigan. Customers can still use their cards at all locations; however, they do this by selecting the “debit” option and entering the PIN code. The bank has experienced “minor impacts” from the situation, the vice president said, but he declined further comment.


23. *June 15, Bank Info Security* – (Pennsylvania) **Ex-Teller guilty of insider scheme.** In the latest example of insider fraud, a former JPMorgan Chase employee pleaded guilty to participating in a scheme to steal more than $60,000 from New Jersey bank customers’ accounts. The 22-year-old suspect, of Sciota, Pennsylvania, admitted that she took part in the scheme in 2008 and 2009. As a teller at the JPMorgan Chase bank in Hackettstown, New Jersey, according to a release from the U.S. Department of Justice, the suspect accessed 12 customer account profiles and sold them to two people in Monroe County, Pennsylvania. The two individuals used the information to have false identification documents made, and used those credentials to access the accounts. The other two suspects have already pleaded guilty to bank fraud and attempted bank fraud as aiders and abettors. They are awaiting sentencing. The former Chase employee was charged in a complaint filed by the United States Attorney’s Office in April 2010. Her charge resulted from an investigation conducted by the FBI and Hackettstown police. The U.S.attorney for the Middle District of Pennsylvania said that as a result of
the guilty plea, the suspect faces up to 10 years in prison and a $250,000 fine. She will be sentenced September 8.

**Transportation Sector**

24. *June 18, NBC 4 New York* – (International) **El Al Airline scare as fake ‘plastic explosives’ make it to JFK.** A lifelike, fake plastic explosive, apparently used for bomb training at Israeli airports, was accidentally left on board an El Al plane after an exercise there, and made its way aboard a passenger flight to New York, officials said. The diplomatic pouch traveled from Israel to New York — and then wound up being delivered to the Israeli Consulate on Manhattan’s east side. The devices were inert, police said. Israeli consulate officials apparently tried to send the pouch back to Ben Gurion Airport, and it sat in a JFK airport office for several days. When it finally was set to be returned overseas on an El Al flight, it set off alarms at JFK airport. Port Authority and New York police were called to investigate. Airport officials said the mix-up appears to have been an initial mistake by a security official in Israel who left the pouch behind. The fake devices were made of clay, but were meant to look like a sophisticated plastic explosive.

25. *June 17, WBTV 3 Charlotte* – (North Carolina) **Charlotte train station evacuated, bomb squad called out.** A Charlotte, North Carolina Amtrak station was evacuated June 17 after a suspicious item was found on a train. An Amtrak spokeswoman said Norfolk Southern police asked them to evacuate the entire facility after the suspicious items were found on top of three tankers aboard a train around 10:30 a.m. Thursday. Police officers and the bomb squad were called to the Charlotte Amtrak station to help in the investigation. The affected train was Train 73 from Raleigh to Charlotte, which had 47 passengers on board.

26. *June 17, Seward City News* – (Alaska) **Railroad to begin herbicide spraying after nearly three decades.** Alaska Railroad Corp. has received a permit from state regulators to spray the herbicide AquaMaster (Glyphosate) and Agri-Dex, a substance to help spread it, along 30 miles of track between Seward and Indian. The railroad has not used chemical weed control for the past 26 years due to widespread public opposition, and an inability to obtain the needed permits. The Alaska Department of Environmental Conservation (DEC) permit is for two years. But earlier this month, six Alaska environmental groups and the Native Village of Eklutna intervened to delay DEC from activating the permit. The groups are hoping that the agency will reverse its decision altogether. “The Alaska Railroad does not take the use of an herbicide lightly,” stated an ARRC spokeswoman in an e-mail to SewardCityNews.com. “After spending considerable resources and time trying to control weeds without the use of herbicides,
the railroad has continued to lose ground,” she said. Last year, the Federal Railroad Administration (FRA) issued 130 vegetation-related violations to ARRC for failing to meet federal-safety mandates with regard to vegetation in and around the tracks. These carry potential fines of $1,000 apiece. As recently as late May, FRA inspectors returned, and issued 20 additional violations for vegetation. FRA warned the railroad that its safety situation was critical and needed be corrected. They said if the problem isn’t addressed, they could be forced to slow down the trains, or close the tracks in certain areas. The railroad said it fears trains could derail. Alaska’s train system carries nearly 500,000 passengers a year, and approximately 40 percent of its freight is classified as hazardous materials.


For more stories, see items 5, 7, 13, 34, 37, and 62

Postal and Shipping Sector

Nothing to report

Agriculture and Food Sector

27. June 17, Alton Telegraph – (Illinois) Bomb threat closes Jerseyville grocery. The Sinclair Food Mart, a full-line grocery store in Jerseyville, Illinois, was emptied and closed June 17 because of a bomb threat. A witness said police closed the store and the street that runs next to the establishment. The witness said police had cleared the area and reopened the streets between 4:30 and 5 p.m. A dispatcher for the Jerseyville Police Department said that a police chief would be issuing a news release on the incident later. However, no news release had been issued as of 8 p.m.


28. June 17, U.S. Food Safety and Inspection Service – (Texas; National) Texas firm recalls three varieties of ‘SpaghettiOs’. Campbell Soup Supply Company is recalling approximately 15 million pounds of “SpaghettiOs with Meatballs” canned products due to possible under-processing, the U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS) announced June 17. The following products are subject to recall: 14.75-ounce cans of “SpaghettiOs” with Meatballs, bearing the identifying product code “U5” on the bottom of the can; 14.75-ounce cans of “SpaghettiOs” A to Z with Meatballs, bearing the identifying product code “4N” on the bottom of the can; 14.75-ounce cans of “SpaghettiOs” Fun Shapes with Meatballs (Cars), bearing the identifying product code “KS” on the bottom of the can. The problem was discovered through a routine warehouse inspection by the company and its subsequent investigation. FSIS has received no reports of illnesses from consumption of these
products.
Source:

29. June 17, U.S. Food Safety and Inspection Service – (National) **Iowa firm recalls frozen chicken products due to possible salmonella contamination.** ConAgra Foods Packaged Foods is recalling Marie Callender’s brand Cheesy Chicken and Rice frozen meals, the U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS) announced June 17. The product subject to recall include: 13-ounce packages of “Marie Callender’s Cheesy Chicken & Rice White Meat Chicken and Broccoli over Rice Topped with Rich Cheddar Sauce.” The company is recalling all meals in commerce, regardless of production date. These products are being recalled after the company was informed by the U.S. Centers for Disease Control and Prevention (CDC) of an investigation involving 29 people in 14 states who have been diagnosed with salmonellosis linked to Salmonella serotype Chester. Eight of the patients specifically reported eating this product in April and May 2010, prior to illness onset; the last reported illness was reported May 22. FSIS became aware of the problem during the course of an ongoing investigation of a multi-state outbreak of Salmonella serotype Chester illnesses. CDC, the Food and Drug Administration (FDA), FSIS, and state health and agriculture departments are cooperating in this ongoing investigation.
Source:

30. June 16, Daily Comet – (Louisiana) **Coast Guard seizes 19,000 pounds of shrimp caught in closed fishery.** About 19,000 pounds of shrimp were seized June 12 from a Panama City, Florida boat trawling in federal water 13 miles south of Belle Pass, Louisiana that was closed because of the oil spill, the U.S. Coast Guard said. The National Oceanic and Atmospheric Administration (NOAA) is reviewing the case to determine whether a citation will be issued. NOAA and Coast Guard authorities said the case is the first investigation of a fishing violation in federal waters since the April 20 Deepwater Horizon explosion. The Coast Guard dumped the load of white shrimp back into the water, according to a petty officer. A sample of the shrimp was also taken for testing. He is unsure whether the captain of the Little Andrew was intentionally fishing in the restricted area or whether he was unaware the area is closed. About 32 percent — or 78,264 square miles — of the 242,014 square miles of federal water in the Gulf of Mexico is closed, according to NOAA. A spokeswoman for the Louisiana Seafood Promotion and Marketing Board said about 70 percent of the coast remains open to fishing. Most fishermen have refrained from working to avoid the risk of allowing contaminated product from entering the market. She said no Louisiana seafood has tested positive for hydrocarbons.
Source:
Water Sector

31. *June 18, Lansdale Reporter* – (Pennsylvania) **Meat plant fined $8m for waste water violations.** JBS Souderton Inc., which was known as Smithfield Beef Group prior to October 23, 2008, must pay at least $8 million in civil penalties and for upgrades to its Franconia plant operation and maintenance. That is part of a settlement announced Wednesday with the U.S. Environmental Protection Agency (EPA) and Pennsylvania. JBS entered into a consent decree after failing to comply with the Clean Water Act during plant operations, which resulted in fish kills August 10, 2007; December 5, 2007; and June 10, 2008. A total of 24,715 fish were killed in those incidents, according to the U.S. Department of Justice. “The Souderton facility is in full compliance with wastewater discharge requirements as we speak,” said a JBS spokesman. “These problems predated the purchase of this plant by JBS,” he said. Water from the beef processing and rendering facilities is conveyed to an on-site wastewater treatment plant, treated, and then discharged into the Skippack Creek. JBS must reconstruct its wastewater system and spend $6 million on a new wastewater treatment plant, according to the Department of Justice. The spokesman said those upgrades have already been completed. A wastewater piping upgrade where they are doublewalling pipes to prevent leaks will be done by this month, he said. The corporation must also pay $1.9 million in penalties, and $100,000 in damages.


32. *June 17, U.S. Environmental Protection Agency* – (Mississippi) **Pontotoc Union Lee Alliance ordered to pay $70,000 in penalties for stormwater violations in Blue Springs, Miss.** The U.S. Environmental Protection Agency (EPA) recently settled with Pontotoc Union Lee Alliance (PULA) for stormwater-related violations of the Clean Water Act at two of its construction sites in Blue Springs, Mississippi. Under the terms of two separate Consent Agreements and Final Orders, PULA has agreed to come into compliance and paid penalties totaling $70,000. PULA, along with Eutaw Construction Company, Inc., entered a $40,000 settlement with EPA for stormwater violations at its construction site known as Blue Springs Rail Spur. And PULA, along with L&T Construction, Inc., entered a separate $30,000 settlement with EPA for stormwater violations at its construction site known as Blue Springs North Loop Interchange. Both settlements stem from violations that were observed by representatives from EPA and the Mississippi Department of Environmental Quality during May 2009 inspections of the construction sites. EPA issued Administrative Orders in October 2009 requiring the violators to revise their Notices of Intent for Permit coverage, modify their Stormwater Pollution Prevention Plans, institute inspection programs, and address areas of potential discharges. The companies have complied with EPA’s enforcement order.

Source: [http://yosemite.epa.gov/opa/admpress.nsf/e77fdd4f5afdf88a3852576b3005a604f/ea871eadc1248b9a8525774500466f2c!OpenDocument](http://yosemite.epa.gov/opa/admpress.nsf/e77fdd4f5afdf88a3852576b3005a604f/ea871eadc1248b9a8525774500466f2c!OpenDocument)
33. *June 17, Philadelphia Inquirer* – (Pennsylvania) **Water main breaks, becomes a geyser in N.E. Phila.** A water main broke the morning of June 17 in Northeast Philadelphia, creating a geyser visible to motorists on I-95. Water shot 60 feet into the air after a contractor cracked a 24-inch main while working on a project in the Upper Holmesburg section. The unusual sight caused backups in the area of I-95. About 2 million gallons were lost before crews shut the gusher down about 8:15 a.m., a spokeswoman for the Philadelphia Water Department said. The transmission main, made of ductile iron, was punctured by a drill rig operating on State Road near Pennypack Street. The break caused low-water pressure for about 90 minutes in the Somerton section but no customers lost service. The break was in front of the Philadelphia Water Department’s Samuel S. Baxter Water Treatment Plan, and near the police department and fire department academies.


34. *June 17, WSB 750 Atlanta* – (Georgia) **Main break causes Atlanta sinkhole.** A southwest Atlanta, Georgia, neighborhood has been cut off to vehicle traffic by a water main break that caused several sinkholes along Empire Boulevard near its intersection with Old Hapeville Road. The Atlanta Department of Watershed Management has notified affected residents in about 30 houses in the area that it could take repair crews several days to shore up the roadway and replace piping. The street collapsed around 5 p.m. Wednesday when a fire hydrant separated from a water main, releasing thousands of gallons of water that eroded the pavement. Until the repairs are complete, access into and out of the neighborhood is limited to walking.


35. *June 17, KTTS 94.7 Springfield* – (Missouri) **Sewage leak in Finley River.** About 162,000 gallons of partially treated sewage has leaked from the wastewater treatment facility in Ozark, Missouri. The state’s department of natural resources said it was caused by a power outage. The sewage poured into the Finley River, and the city will be sampling the water until results are normal. Officials said people should not swim in the river.


36. *June 17, U.S. Environmental Protection Agency* – (National) **EPA proposes updating drinking water rule to better protect public health.** The U.S. Environmental Protection Agency (EPA) is proposing to revise a national primary drinking water regulation to achieve greater public health protection against waterborne pathogens in the distribution systems of public water systems. EPA is proposing to revise the 1989 Total Coliform Rule to incorporate improvements recommended by a federal advisory committee. The revised rule will better protect people from potential exposure to dangerous microbes because it requires water systems to take action when monitoring results indicate that contamination or a pathway to contamination may be present. The proposal also provides incentives for better system operation by improving the criteria for public water systems to qualify for and stay on reduced monitoring, which provides
an opportunity to reduce system burden. In addition, the proposed rule updates conditions that will trigger public notices to better represent the relative health threat identified. It also makes the wording required in these public notices more clear. EPA is seeking public comment on this proposed rule for 60 days following publication in the Federal Register.
Source: http://yosemite.epa.gov/opa/admpress.nsf/0/2E4503668A34B3DD852577450061A0C8

Public Health and Healthcare Sector

37. June 17, KLRT 16 Little Rock – (Arkansas) Human heads found in packaging at Little Rock Airport. A Southwest Airlines employee made a startling discovery at the Little Rock National Airport in Little Rock, Arkansas: They found human heads, and lots of them. Now the Pulaski County Coroner is involved. When the airport employee discovered the heads he notified police, who notified the coroner. Now, the coroner said he is going to hold onto the heads while he investigates the odd discovery. It all started when Conway company JLS Consulting Group LLC attempted to ship 30-60 human body parts via Southwest. The packages raised employee eyebrows because they were labeled incorrectly. It caused the employees to open the containers only to find the human heads inside. The company shipping the parts said they were headed to Fort Worth, Texas. Company officials said they had every right to send the heads. They said they were actually being sent to doctors so they can train with them.
Source: http://www.myeyewitnessnews.com/news/local/story/UPDATE-Human-Heads-Found-In-Packaging-At-Little/hL5YhgJo0uSi0ZPCDr1aQ.cspx

38. June 16, Hagerstown Herald-Mail – (Pennsylvania) Chambersburg hospitals participate in simulation. Chambersburg Hospital and Waynesboro Hospital, non-profit affiliates of Summit Health in Pennsylvania, took part in a Joint Users Interoperability Communications Exercise (JUICE) June 15. The hospitals participated in the simulation to assess their ability to handle a sudden increase in patient volume, demand for supplies and equipment, and to assess their electronic patient tracking systems, according to a news release. “We are involved in simulation exercises like JUICE every year,” said vice president of patient services for Summit Health. “We were very pleased with the outcome of this exercise and our ability to continue to provide top quality care under intense conditions.” Simulated patients suffering from burns and other injuries from an “explosion” flooded the Waynesboro Hospital Emergency Department at around 9 a.m. The simulation extended to Chambersburg Hospital, when employees saw their first “patient” at around 10:30 a.m.
Source: http://www.herald-mail.com/?cmd=displaystory&story_id=247392&format=html

healthcare company, in a press release, said it was recalling the lots after inadvertently failing to include them in a wider recall of over the counter drugs January 15. The company’s McNeil Consumer Healthcare unit said the latest action is a “follow-up” to the recall in January. On that occasion, 53 million bottles of a range of products were recalled after consumers complained of musty or moldy odors. The brands included Tylenol and Motrin painkillers, Rolaids, Benadryl, and St. Joseph’s Aspirin. The drugmaker said the odor that prompted its January 15 recall was linked to traces of a chemical called TBA, caused by the breakdown of a chemical applied to wood used to build pallets that transport and store product-packaging materials. “Further analysis confirms that the risk of serious adverse medical events is remote,” J&J said June 15. J&J said the newly recalled lots — made at a plant in Las Piedras, Puerto Rico — were sold in the United States, Trinidad and Tobago, Bermuda, and Puerto Rico. One of McNeil’s two other main factories, located in Ft. Washington, Pennsylvania, has been shut down while the company strives to fix multiple deficiencies cited by the U.S. Food and Drug Administration.
Source: http://www.reuters.com/article/idUSTRE65E67020100615?type=domesticNews

**Government Facilities Sector**

40. *June 17, Associated Press* – (California) **Police find no explosive in box outside NoHo H.S.** Los Angeles police say no explosives were found in a box that was left in front of North Hollywood High School. The box found outside the school’s front doors early Thursday had wires hanging out. An officer said police determined that the box was harmless after a robotic device was used to investigate it. Police and Los Angeles Unified School District representatives said a custodian discovered the box shortly after 6 a.m. Dozens of arriving students were kept on bleachers at a football field while the robot worked. A district spokeswoman said the school did not receive any bomb threats. She said the campus will hold graduation ceremonies in the evening, but there will be additional security.

41. *June 17, Associated Press* – (International) **2 charged in Mass. with conspiring to aid Al Qaeda.** Two men accused in a terror plot to kill Americans face new federal charges that they conspired to provide personnel, advice, assistance and other services to Al Qaeda. A grand jury Thursday added charges of conspiring to provide material support to a designated foreign terrorist organization in a superseding indictment against a 27-year-old suspect from Sudbury, Massachusetts, and a 28-year-old suspect. Authorities said the 28-year-old suspect, who used to live in Mansfield, Massachusetts, is now in Syria. The men face up to 15 years in prison and a fine of $250,000 if convicted of the latest charge. When reached by phone, the first suspect’s lawyer did not comment. The suspects already face a 10-count indictment. Prosecutors said the men conspired to kill American troops in Iraq, assassinate two unnamed U.S. politicians, and shoot shoppers in U.S. malls.
42. June 17, Fox News – (National) Alert issued for 17 Afghan military members AWOL from U.S. air force base. A nationwide alert has been issued for 17 members of the Afghan military who have gone AWOL from an Air Force base in Texas where foreign military officers who are training to become pilots are taught English, FoxNews.com has learned. The Afghan officers and enlisted men have security badges that give them access to secure U.S. defense installations, according to the lookout bulletin, “Afghan Military Deserters in CONUS [Continental U.S.],” written by Naval Criminal Investigative Service in Dallas and obtained by FoxNews.com. The Be-On-the-Lookout (BOLO) bulletin was distributed to local and federal law enforcement officials Wednesday night. The Afghans were attending the Defense Language Institute (DLI) at Lackland Air Force Base in Texas. The DLI program teaches English to military pilot candidates and other Air Force prospects from foreign countries allied with the U.S. “I can confirm that 17 have gone missing from the Defense Language Institute,” said the chief of public affairs, 37th Training Wing, at Lackland AFB. “They disappeared over the course of the last two years, and none in the last three months.”


43. June 17, San Jose Mercury News – (California) Teen arrested after bomb explodes at Menlo Park school field. A 17-year-old boy was arrested late Wednesday night on suspicion of detonating an explosive device near La Entrada Middle School in Menlo Park, California police said. Neighbors called police to report hearing a loud explosion in the Sharon Heights neighborhood at about 10:10 p.m. The teenager was found near the middle school soon after the explosion, and he admitted to detonating a homemade bomb in the grass field directly behind the school, police said. A spokeswoman for the Menlo Park Police Department said the device was possibly a pipe bomb. “The juvenile said he got the materials from a local hardware store,” the spokeswoman said. No injuries or substantial property damage were reported, according to police. The teenager was arrested on suspicion of possessing and detonating an explosive device and cited before being released to his parents, the spokesman said. She described the teenager as cooperative. “He led investigators to believe that he wasn’t trying to cause harm to anybody or any property,” she said. “That’s why he chose that particular time and place to do it.”

Source: http://www.mercurynews.com/breaking-news/ci_15322232?nclick_check=1

44. June 16, U.S. Government Accountability Office – (National) Cybersecurity: Continued attention Is needed to protect federal information systems from evolving threats. Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the federal government. In recent testimony, the Director of National Intelligence highlighted that many nation states, terrorist networks, and organized criminal groups have the capability to target elements of the United States information infrastructure for intelligence collection, intellectual
property theft, or disruption. In July 2009, press accounts reported attacks on Web sites operated by major government agencies. The ever-increasing dependence of federal agencies on information systems to carry out essential, everyday operations can make them vulnerable to an array of cyber-based risks. Thus it is increasingly important that the federal government carry out a concerted effort to safeguard its systems and the information they contain. GAO is providing a statement describing (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies that make federal systems vulnerable to those threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement, GAO relied on its previously published work in this area.

Source: http://www.gao.gov/products/GAO-10-834T

45. June 16, Infosecurity – (National) **Social Security flexible workplace program leaves personal data at risk.** The Social Security Administration’s (SSA) Inspector General recently issued his report evaluating the agency’s new flexible workplace program (known as Flexiplace) that was negotiated between the SSA and unions representing the agency’s Office of Disability Adjudication and Review (ODAR) staff. The program permits hearing officers to conduct evaluations from an alternate site one day per week, usually the employee’s home, and while the audit showed an increase in worker morale and increased productivity, the IG also warned the SSA that these employees routinely put beneficiary data at risk through a variety of means. Files used by ODAR staff routinely contain Social Security numbers, names, addresses, and a wealth of other personal data. The IG audit results come from interviews of 135 hearing officers and 75 ODAR managers since the implementation of Flexiplace and found that ODAR employees had transported personal identifying information (PII) files from its facilities using unencrypted CDs, in addition to improper chain of custody documentation when removing and returning files containing PII. “While SSA had implemented some preventative measures to safeguard PII removed from its premises, we determined ODAR practices may have exposed claimant data to unauthorized disclosure”, noted the report. “We believe ODAR should identify opportunities to better monitor employee compliance and strengthen Flexiplace controls.”


46. June 15, Washington Technology – (National) **L-3 division accused of snooping through e-mail.** The Air Force is investigating allegations that a division of L-3 Communications Inc. read e-mail messages of employees, government workers and other contractors. The unit, Special Support Programs Division, has been barred from new federal contracts or orders, according to Bloomberg Businessweek, which quoted an Air Force memo. L-3 managed the military network and copied and stored e-mail messages to collect information on upcoming competitions, Businessweek reported. The company is cooperating with the investigation, a spokesman told the magazine. L-3 is ranked No. 8 on the 2010 Washington Technology Top 100 list of the largest government contractors.

Emergency Services Sector

47. June 17, ANSI-ASQ National Accreditation Board – (National) Standards announced for private sector preparedness. The Department of Homeland Security (DHS) announcement of adoption of standards for the Voluntary Private Sector Preparedness Accreditation and Certification (PS-Prep) program marks a major milestone. Under an agreement with DHS, the ANSI-ASQ National Accreditation Board will be the accreditation body for the PS-Prep Program. Accreditation will be offered under the ANSI-ASQ National Accreditation Board’s ANAB brand. “Private organizations across the country — from businesses to universities to non-profit organizations — have a vital role to play in bolstering our disaster preparedness and response capabilities,” the DHS Secretary said. “These new standards will provide our private sector partners with the tools they need to enhance the readiness and resiliency of our nation.” The adoption of the standards — developed by the National Fire Protection Association, the British Standards Institution, and ASIS International — was published in a June 16, 2010, Federal Register notice following a series of regional public meetings and the incorporation of public comments. Source: http://www.wisbusiness.com/index.iml?Article=200246

48. June 17, Richmond Times-Dispatch – (Virginia) Parham Road reopened; ‘suspicious’ vehicle was outside FBI office. Authorities Thursday evening shut down part of East Parham Road in Richmond, Virginia after what police described as a “suspicious situation” outside the FBI field office in Henrico County. Someone apparently parked a vehicle beside a guard booth at the field office in the 1900 block of East Parham Road after regular working hours, and then walked away along Parham, said an FBI spokeswoman. Henrico police were summoned shortly after 7 p.m. and shut down Parham from Woodman Road to Lydell Drive for about an hour. Henrico and FBI bomb technicians determined that the parked vehicle posed no threat, and it was towed away. The FBI spokeswoman said she did not know why the person parked there. No arrest has been made. Source: http://www2.timesdispatch.com/rtd/news/local/article/FBIIGAT17_20100617-220002/351810/

49. June 16, The Herald-Bulletin – (Indiana) Communications network may need multimillion fix. Indiana’s statewide wireless public-safety communications network, created to connect emergency responders in a crisis, is near capacity and may need a multimillion-dollar fix. The network, known as Project Hoosier Safe-T, is used by more than 900 public safety organizations, ranging from rural volunteer fire departments to the global security group at pharmaceutical giant Eli Lilly and Co. That translates to more than 52,000 registered users, bringing the system to near capacity at a time when requests to participate continue to grow. “We expect to be at our maximum number of users soon,” said executive director of the Indiana Integrated Public Safety Commission, or IPSC, which oversees the network. Project Hoosier Safe-T is a wireless communications system that employs technology to create interoperability. It
allows emergency responders that use different radio systems to communicate quickly in a crisis. 

Information Technology Sector

50. **June 18, V3.co.uk** – (International) **Anti-vuvuzela trumpet software is a scam.** Security experts are warning World Cup fans not to fall for a piece of scam software promising to remove the noise of the South African vuvuzela trumpets during TV broadcasts. Links to a Web site selling the ‘Anti-Vuvuzela Filter’ have been making the rounds on various social networks this week, but a Webroot malware researcher said that the 2.95 Euro price tag will leave users with nothing but an empty wallet. “The site claims to be able to ‘get rid of the vuvuzela noise through active noise cancellation’ but all you get for your money is, apparently, a 45-minute MP3 file,” he wrote in a blog post. “Seriously. Call it a rogue AV (anti-vuvuzela) of a variety we haven’t seen before. Don’t be a sucker. Just reduce the volume on your TV if the vuvuzelas get you down.” The scam is the latest in a string of attempts by cyber criminals to extort money by using the World Cup as a lure. Trend Micro and Symantec Hosted Services have both alerted users to Nigerian e-mail scams, while Symantec warned of more sophisticated information stealing malware using the World Cup to target specific corporate systems.

51. **June 18, IDG News Service** – (International) **Google Wi-Fi data grab snared passwords, e-mail.** Wi-Fi traffic intercepted by Google’s Street View cars included passwords and e-mail, according to the French National Commission on Computing and Liberty (CNIL). CNIL launched an investigation last month into Google’s recording of traffic carried over unencrypted Wi-Fi networks, and has begun examining the data Google handed over as part of that investigation. Google revealed May 14 that the fleet of vehicles it operates to compile panoramic images of city streets for its Google Maps site had inadvertently recorded traffic from unencrypted Wi-Fi networks. Google’s intention was only to record the identity and position of Wi-Fi hotspots in order to power a location service it operates, the company said. However, the software it used to record that information went much further, intercepting and storing data packets too. At the time, Google said it only collected “fragments” of personal Web traffic as it passed by, because its Wi-Fi equipment automatically changes channels five times a second. However, with Wi-Fi networks operating at up to 54M bits per second, it always seemed likely that those one-fifth of a second recordings would contain more than just “fragments” of personal data. That has now been confirmed by CNIL, which since June 4 has been examining Wi-Fi traffic and other data provided by Google on two hard disks, and over a secure data connection to its servers. Data-protection authorities in Spain and Germany have also asked Google for access to Wi-Fi traffic data intercepted in their countries, but the CNIL was the first to have its request
granted, it said.
Source:
http://www.computerworld.com/s/article/9178220/Google_Wi_Fi_data_grab_snared_passwords_e_mail

52. June 18, SC Magazine – (International) Kaspersky Lab: Mobile malware evolves as an industry focus on it is the next step. The threat of malware and botnets for mobile phones could become as much of a problem as they are for PCs. The mobile research group manager and senior analyst at Kaspersky Lab pointed at threats such as the “brother” and “Ikee” worms, and said that it was now seeing 30 developments a month in mobile malware, and 35 percent of malware is now designed to infect mobile Internet. He said: “This threat will not go away, and the reasons for the whole Internet-based malware appearance is that new technologies will be the future. A mobile botnet will have the same impact as a simple PC botnet. They will be able to send SMS, MMS, Google spam and mask passwords, and maybe provide telephone DDoS attacks. Imagine a big organization and they have four main telephone numbers, and the competitor does not want to work honestly and decides to do bad things such as a telephone DDoS. Imagine all of the smartphones all started to dial four numbers, and will always be busy so users will have no chance to dial and the company will not be able to do anything.” Asked about the specific threats for mobiles, the analyst told SC Magazine that the threats are more Web-based and are mainly Trojans. He said: “Cyber criminals try to mask applications to download software, so when people use computers for downloading software for mobile, that is how we detect Trojan programs.”
Source: http://www.scmagazineuk.com/kaspersky-lab-mobile-malware-evolves-as-an-industry-focus-on-it-is-the-next-step/article/172738/

53. June 17, The Register – (International) Researcher shows how to strike back at web assailants. A security researcher has disclosed details on more than a dozen previously unknown vulnerabilities that people responding to Web-based attacks can exploit to strike back at online assailants. The bugs reside in off-the-shelf crimeware kits that go by names such as Eleonore, Liberty, Neon, and Yes. Attackers install them on compromised Web sites to streamline the process of exploiting unpatched vulnerabilities on the PCs of people who visit them. It has long been known that some of the exploit kits are themselves susceptible to attacks, and June 17 the CEO of French security consultancy Tehtri-Security detailed 13 bugs that can be exploited to turn the tables on the criminals running the software. They make it possible for law enforcement agents and other investigators of online attacks to destroy command and control servers, identify the miscreants, and in some cases even launch client-side attacks against the intruders. “The offensive concepts that we’ve shown today were how to strike back at attackers who use evil Web tools like exploit packs, Web backdoors, etc.,” the CEO told The Register in an online discussion a few hours after he made a presentation at the SyScan security conference in Singapore. “Basically, we explained that it is possible to create traps or to remotely attack the malicious Web tools used by people controlling botnets.” One of the attacks against Eleonore allows investigators to steal the authentication cookies of miscreants logging in to the administrative panel used to control an attack site. It starts with as SQL-injection

- 22 -
exploit through a browser’s referrer field to plant strings in the server’s database that make the panel vulnerable to XSS, or cross-site scripting exploits. Investigators can then exploit that hole and steal the cookies, which are used to gain administrative access to the panel.

Source: http://www.theregister.co.uk/2010/06/17/exploiting_online_attackers/

54. June 17, DarkReading – (International) Cybersecurity not a ‘Command And Control’ effort. Cybersecurity initiatives will always be distributed efforts, which is what makes the cybersecurity czar’s position so crucial, according to the Department of Homeland Security’s cybersecurity director. “This is not a command and control environment,” said the director of the National Cybersecurity Center at DHS, in an interview June 17. “DoD has key responsibilities, DHS has key responsibilities, and so do the Department of Commerce and NIST, which is part of Commerce. And there are multiple entities in the private sector [with responsibilities as well].” With the flurry of activity on Capitol Hill these days over cybersecurity legislation and the recent formation of the U.S. Cyber Command, the U.S.’s cybersecurity policy and efforts are getting difficult to pin down. But the director said that is where the administration’s cybersecurity coordinator comes in. “Cybersecurity has always been distributed and will remain distributed,” he said. The administration is getting close to actually testing out its newest cyberincident-response plan. The DHS will sponsor the CyberStorm III cybersecurity drill in September, which will put the nation’s new cyber response plan through its paces in a simulated attack scenario to see if it is on the mark and whether it needs any tweaks. This simulation will be different from previous ones because it will include international players. “Cybercrime is inherently international,” the director said. “Even if someone in the U.S. is breaking into another system in the U.S., the chances are that communication is going to go internationally.”

Source: http://www.darkreading.com/security/government/showArticle.jhtml?articleID=225700567

For another story, see item 56

Internet Alert Dashboard

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

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

Communications Sector

55. June 18, InformationWeek – (International) FCC considers broadband regulation. Major high-technology providers are divided over the Federal Communication Commison’s (FCC) plan — approved in a 3-2 vote Thursday — to
consider the reregulation of Internet broadband. The big three broadband carriers — AT&T, Comcast and Verizon — issued statements opposing the FCC’s decision to conduct an inquiry into whether broadband should be classified as a telecommunications service, giving the FCC more regulatory power over the carriers. Content providers like Amazon, Google and Skype, however, favored the FCC action. On the other side of the issue is the Open Internet Coalition whose members include Amazon, eBay, Google, and Skype. The coalition’s executive director said: “There is a real urgency to this because right now there are no rules of the road to protect consumers from even the most egregious discriminatory behavior by telephone and cable companies.”


56. June 15, Federal Computer Week – (International) Internet gatekeepers strengthen security at the root. The Commerce Department and global Internet authorities will begin deploying a worldwide root-system improvement to the Internet designed to enhance security in the Internet’s domain name structure. The Internet Corporation for Assigned Names and Numbers will host a ceremony June 16 at a high-security data center in Culpeper, Virginia, to install the first Domain Name System Security Extensions. During the ceremony in Virginia, the first cryptographic digital key used to secure the Internet root zone will be generated and securely stored, according to a news release. Official procedures will be carried out to assure the security of the key. The security-extensions system is a cryptographic framework that provides greater assurance to all Internet users so that, when they type in a Web address, there is more confidence they will reach that destination. The security extensions have been in development for more than a year to address a well-known flaw in the Internet that has been exploited by hackers and phishers. The longstanding domain name vulnerability has allowed hackers to misdirect Internet traffic to malicious Web sites.


Commercial Facilities Sector

57. June 18, Los Angeles Times – (California) Despite heavy LAPD presence, violence breaks out after Lakers’ victory. Sporadic violence broke out near Staples Center in Los Angeles after the Lakers defeated the Boston Celtics in the National Basketball Association finals June 17. As the Lakers battled the Celtics in the first half, crowds began to form at the Nokia Theatre plaza across from Staples Center. Witnesses said the Los Angeles Police Department (LAPD) was quick to respond when the throng began to grow. Crowds hurled bottles and other objects at police, smashed marquees, jumped on vehicles, broke windows, and set rubbish dumpsters and vehicles on fire along Figueroa Street north of Staples Center and on Flower Street. Police fired non-lethal rounds to disperse the crowd at Figueroa and Venice Boulevard after several
small fires were set, as well as at 11th and Hope streets. At 7th and Flower, a car believed to be a taxicab was engulfed in flames. At least one person was beaten unconscious as fights broke out on Flower Street near Olympic Boulevard. A bicyclist was injured when struck by a Los Angeles County Sheriff’s Department vehicle near 11th and Flower streets. In all, there were multiple injuries but no loss of life. One police officer suffered a broken nose. As the night wore on, fire crews responded to many rubbish fires and some vehicle fires, according to the Los Angeles Fire Department. The LAPD declared an unlawful assembly moments after the game ended. Hundreds of officers in patrol cars, on foot and on horseback moved in to clear streets and break up crowds. At least 12 people were arrested for crimes including public drunkenness, vandalism, and inciting a riot. One person was arrested for assault on a police officer. The LAPD reported things seemed to be calming down after 11 p.m.

Source: [http://www.wqad.com/sports/la-me-0618-lakers-20100618,0,7141877.story](http://www.wqad.com/sports/la-me-0618-lakers-20100618,0,7141877.story)

58. *June 17, KGUN 9 Tucson* – (Arizona) **Bomb threat at Ronstadt Center.** Police are investigating a call of a bomb threat at the Ronstadt Center in downtown Tucson, Arizona. The Tucson Police Department said they received a call at 5:03 p.m. June 17 from a telephone number outside the area reporting that there was a bomb at the center. Officers are searching the property for suspicious devices. Traffic is not being restricted at this time.


59. *June 17, KLEW 3 Lewiston* – (Idaho) **Bomb squad called to north Lewiston storage unit.** An improvised explosive device was found in North Lewiston, Idaho at the 7th Avenue North Mini Storage, June 17. The circular cylinder was detonated by Spokane County Bomb Disposal. Idaho State Police are investigating the case along with the Nez Perce County Sheriff’s Office. They are not releasing the name of the owner of the storage unit or how they pinpointed the location.


60. *June 17, KCAL 9 Los Angeles* – (California) **Explosion kills 1, injures 3 in Simi Valley.** An explosion has killed one person and injured three others at a business in a Simi Valley, California industrial area. Simi Valley firefighters responded to a police call at about 1:15 p.m. June 17. Businesses in a half-mile radius were evacuated. The blast appeared to have punched a hole through the building’s roof. Three people have suffered minor injuries. A fourth person was later found dead at the scene. The cause of the blast is under investigation.


61. *June 16, Associated Press* – (Colorado) **Pipe bomb scare forces evacuation of building.** A reported pipe bomb forced the temporary evacuation of an apartment building about a half mile east of the Colorado State Capitol when an apartment landlord that was evicting tenants found the suspicious device and contacted police June 16. Residents that were home were asked to leave while a bomb squad entered the apartment and rendered the device harmless around noon. Police have started a criminal
investigation.
Source: http://cbs4denver.com/wireapnewsco/Reported.pipe.bomb.2.1755457.html

National Monuments and Icons Sector

62. **June 18, Asheville Citizen-Times** – (North Carolina) **Train spills 3,000 gallons of fuel near Pisgah National Forest.** A derailed train spilled 3,000 gallons of diesel fuel near Pisgah National Forest in Old Fort, North Carolina June 17. Norfolk Southern officials said they were working to mitigate the environmental damage from the morning spill, and they are still trying to determine the cause of the accident. The derailment happened at about 5:40 a.m. in the Mill Creek area eight miles west of Old Fort in McDowell County. No one was injured and no hazardous materials besides the fuel were involved.
Source: http://www.citizen-times.com/article/20100618/NEWS/306180036

63. **June 17, Bureau of Alcohol, Tobacco, Firearms and Explosives** – (California) **ATF offers a reward of $5,000 for information regarding explosives theft.** The Special Agent in Charge of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), San Francisco Field Division and an official with the Siskiyou County Sheriff’s Office announced June 17 that ATF will offer a reward of $5,000 for information leading to the arrest and conviction of those responsible for the theft of explosives that occurred at a United States Department of Agriculture (USDA) Forest Service Site, Shasta-Trinity National Forest in Mount Shasta, California, sometime between the dates of April 12 - April 21, 2010. Since April, 2010, the Siskiyou County Sheriff’s Office and ATF have investigated the theft of the stolen explosives. Investigators said the stolen explosives included 20 Reynolds, RP-83, Exploding Bridgewire Detonators, six Dyno Nobel EZ Det Nonel detonators, and six Austin Powder Rockstar electric detonators. ATF and the Siskiyou County Sheriff’s Office released photographs of the types of the stolen explosives.

For another story, see item 65

Dams Sector

64. **June 18, Associated Press** – (Washington) **Water flowing over Grand Coulee Dam.** So much water is flowing down the Columbia River that it is spilling over the top of the Grand Coulee Dam in Washington. KREM-TV reports that this is the first time since 1997 that dam officials had to lower the floodgates. The water is not currently needed to generate electricity.
65. *June 18, Associated Press* – (Missouri) **Levee breach prompts evacuations in NW Missouri village.** A breach in a farm levee in northwest Missouri has prompted the closing of a state park and voluntary evacuations in the nearby village. Big Lake State Park and the village of Big Lake are located along the Missouri River, about 45 miles north of St. Joseph. The state Department of Public Safety said a 150- to 200-foot section of levee north of Big Lake gave way Thursday morning. Holt County authorities said several hundred acres of farmland were quickly flooded. The village has about 150 year-round residents. Many raised their homes after flooding in previous years. Officials had closed the campground at the state park earlier the week of June 14 as the Missouri River rose. Thursday’s breach led to the closing of the rest of the park.

Source: http://www.newstribune.com/articles/2010/06/18/news_state/nt196state48biglake10.txt

66. *June 18, KXLF 4 Butte* – (Montana) **Water seeping through dam at the Basin Creek Reservoir.** The recent rain combined with runoff from the Highland Mountains south of Butte, Montana has forced water to seep through the dam at the Basin Creek Reservoir. The water washed out a ditch at the site. The area dried up after the flood gates were open, the manager for water treatment for Butte-Silver Bow said. Water from the reservoir is gushing out. He said the recent rain combined with runoff brought the water level close to full pool. But once the gates were opened, the level dropped by a foot and a half within 24 hours. The integrity of the dam was never compromised, he said. However, with the gates open, the creek is running high with water flowing over this portion of the road downstream. Workers are also keeping a close eye on the culverts and said they are in good shape. The dam was built in 1890. It was inspected in 2006 and that is when a new spill wall was installed. Just east of the reservoir, city county workers were busy repairing a section of Roosevelt Drive off of Highway 2 where the stretch of road was starting to crumble into the rushing waters of Blacktail Creek. Workers were filling in the washed out section with boulders, sand and gravel.


67. *June 17, Associated Press* – (Washington) **Repair planned for Chehalis River’s Airport Levee.** The U.S. Army Corps of Engineers and the Chehalis-Centralia Airport will begin repairs June 28 on Airport Levee near the Chehalis River in Chehalis, Washington. The levee protects the airport, a number of commercial buildings and some homes from the Chehalis River, and also keeps flood waters away from a portion of Interstate 5. The levee was damaged in the January 2009 flood. The project, expected to cost nearly $500,000, involves rebuilding more than 5,000 feet of the levee. Work is expected to be finished in late July or early August. The Corps and the airport are partnering to pay for the project with the Corps paying 80 percent of the cost.

DHS Daily Open Source Infrastructure Report Contact Information

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

**Contact Information**

<table>
<thead>
<tr>
<th>Content and Suggestions:</th>
<th>Send mail to <a href="mailto:NICCReports@dhs.gov">NICCReports@dhs.gov</a> or contact the DHS Daily Report Team at (202) 312-3421</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribe to the Distribution List:</td>
<td>Visit the <a href="http://www.dhs.gov/iaipdailyreport">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="http://www.dhs.gov/iaipdailyreport">Get e-mail updates when this information changes.</a></td>
</tr>
<tr>
<td>Removal from Distribution List:</td>
<td>Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a>.</td>
</tr>
</tbody>
</table>

---

**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](http://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.