



Homeland Security

Daily Open Source Infrastructure Report for 28 June 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- Associated Press reports that Boeing said it is likely to recommend more inspections for some of its 767s after American Airlines found cracks where the engine attaches to the wing. Boeing is considering asking airlines to inspect the wings every 400 flights, a spokesman said Thursday. (See item [25](#))
- At least 11 of the 17 members of the Afghan military who went AWOL from an Air Force base in Texas have turned up on Facebook, according to Fox News. Some belong to the “Afghanistan Mujahideen” group, a page that features, among other content, videos from the American-born al Qaeda spokesman Azzam the American. (See item [37](#))

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 25, msnbc.com, NBC News, Reuters and Associated Press* – (Louisiana) **Storm system may slam Gulf, BP cleanup sites.** On June 25, beleaguered officials in New Orleans were bracing for a tropical storm that could descend on the Gulf of Mexico within the next 48 hours, and delay oil spill recovery efforts in the area. The National

Hurricane Center said the morning of June 25 that there is a 70 percent chance that a low-pressure area now developing over the western Caribbean Sea may pick up steam and head toward the Gulf, where oil facilities are clustered, and BP continues to fight back the oil spill. Coast Guard officials told NBC News that they will likely need to remove people from rigs if the storm develops and moves toward south Louisiana — a process that they would need to begin five days before the storm would hit land. The Coast Guard commandant, who is leading the government’s cleanup efforts in the area, told CNN that officials have begun planning for a worst-case scenario. Oil prices rose in the markets June 25 on news of the impending storm system.

Source: http://www.msnbc.msn.com/id/37921094/ns/disaster_in_the_gulf/

2. *June 25, Boston Herald and Associated Press* – (Massachusetts) **2 hurt in Everett Nstar blast.** Federal investigators are probing what caused an explosion that injured two Nstar workers June 24 at an Everett, Massachusetts substation. The Occupational Safety and Health Administration sent an inspector to 173 Alford St. after what Nstar described as a “flash incident” at the substation that connects to the Mystic Power Plant. Two workers were doing maintenance on a circuit about 1:30 p.m. when the massive, faulty electrical current occurred, a Nstar spokeswoman said. Both men were taken to Massachusetts General Hospital for non life-threatening injuries. The men were working on equipment that had been bought within the last year. The substation plugs into Nstar’s Charlestown system, which provides electricity to Greater Boston, she said, but no outages were caused by the accident.
Source:
http://news.bostonherald.com/news/regional/view/201006252_hurt_in_everett_nstar_blast/
3. *June 25, Associated Press* – (Northeast) **Bridgeport, Conn., views damage from strong storm.** A severe storm tore through Bridgeport, Connecticut June 24, toppling trees and power lines and collapsing several buildings as part of a powerful line of storms sweeping across parts of the Northeast. Hundreds of bricks shook loose from buildings, trees split in half and crushed cars, and a billboard hung precariously several stories up over Main Street in Bridgeport. Nine buildings were partially or fully collapsed, including at least three that were brought to their foundations. Rescuers searched the rubble to ensure no one had been inside. High winds from the system knocked out power to tens thousands of customers from Maine to Pennsylvania. Philadelphia-based utility Peco said 155,000 customers were without power the morning of June 25. In Bridgeport, the mayor declared a state of emergency. He said another 20 to 30 buildings will have to be inspected and estimated damage in the millions of dollars. A Catholic high school, a museum dedicated to P.T. Barnum, and several other buildings also had roof and window damage. United Illuminating reported nearly 21,100 customers without power after the storms, along with about 3,800 customers of Connecticut Light & Power. The storm contributed to the collapse of a church and a banquet hall in Philadelphia. Winds extensively damaged the roof of a day care center just west of the city.

Source:

<http://www.google.com/hostednews/ap/article/ALeqM5gToxGRg5OgeiVpllCklfwJCmigjgD9GIB8I80>

4. *June 24, Platts* – (National) **US PHMSA promises extra scrutiny of BP onshore oil, gas pipelines.** The U.S. Pipeline and Hazardous Materials Safety Administration (PHMSA) has given extra scrutiny to BP's network of onshore oil and gas pipelines in light of the Deepwater Horizon disaster, the department's head told a Senate panel Thursday. The PHMSA Administrator told the Senate Committee on Commerce, Science and Transportation that she recently met with the president of BP Pipelines and "explained to him that we would be looking very closely at their program and doing an integrated inspection of their entire system." The chairman of the National Transportation Safety Board said the Liberty project and the Endicott pipeline deserve attention. "We would want to make sure that they have adequate remote control shutoff valves, that they have corrosion protection, that the pipeline is marked," she said. A Texas Senator asked whether two deadly natural pipeline blasts this month in her state demonstrate the need for more efforts to prevent excavation accidents, in particular. The PHMSA Administrator said both accidents were "absolutely preventable" and that more work needs to be done on public awareness, pipeline markings and other safety measures.

Source:

<http://www.platts.com/RSSFeedDetailedNews.aspx?xmlpath=RSSFeed/HeadlineNews/Oil/6140414.xml>

5. *June 24, NewsOK* – (Oklahoma) **Oil spill in Oklahoma City river may take days to clean up.** Cleanup from an oil spill into the Deep Fork of the Canadian River found June 21 by a bridge inspector is expected to continue into the week of June 28. The 250-barrel leak happened two miles south of Arcadia Lake in Oklahoma City, Oklahoma. An Oklahoma County field inspector for the Oklahoma Corporation Commission said the oil leak came from a pipeline that had been abandoned for decades. The leak has been sealed and the spill has been contained. The leak was found by a department of transportation bridge inspector where the Deep Fork flows under Britton Road. Workers from Duke Conoco-Phillips, which does not own the pipeline, traced the leak to a pipeline near Wilshire Road and Interstate 35. "It had a small pinhole in it leaking oil into the river," the inspector said. "It was 8,000 feet long from point of origin, but because of the slow-moving current, it was easily contained." The Environmental Protection Agency (EPA) is coordinating the cleanup using skimmers, containment and absorbing booms, pumps and a vacuum truck. An EPA spokesman said the agency is looking for the owner of the leaky pipeline. The Edmond Water Resources superintendent said he does not think the amount of oil spilled will have any effect on drinking water.

Source: http://www.newsok.com/oil-spill-in-oklahoma-city-river-may-take-days-to-clean-up/article/3470683?custom_click=headlines_widget

6. *June 23, Nextgov* – (Louisiana) **Government delayed measuring rate of oil flow for five weeks.** The federal government delayed by five weeks deploying high-tech sensors that could accurately measure the how much oil was spewing out of the BP well in the

Gulf of Mexico because officials thought the well would be capped or shut down within a relatively short time span, according to contract documents the U.S. Coast Guard released June 21. The National Atmospheric and Oceanic Administration and BP downplayed the amount of oil gushing into the Gulf, at one time estimating the flow rate was about 5,000 barrels per day after the Deep Horizon drill rig sank April 22. But officials with the Coast Guard Research and Development Center in New London, Connecticut decided May 26 they needed an accurate assessment because BP's estimates "are not consistent with other estimations in the scientific community," they noted in a document titled "Justification for Other Than Full and Open Competition." The week of June 14, the government estimated between 35,000 and 60,000 barrels per day were escaping into the Gulf.

Source: http://www.nextgov.com/nextgov/ng_20100623_9080.php

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

Chemical Industry Sector

7. *June 25, Pryor Daily Times* – (Oklahoma) **Ammonia leak contained in plant.** An anhydrous ammonia leak at Pryor Chemical Company in Pryor, Oklahoma, Thursday was quickly contained, said local officials. Emergency personnel responded to the chemical plant after a pipe ruptured on an ammonia line. The rupture caused an ammonia cloud. The Pryor fire chief said plant personnel diluted the ammonia by spraying large volumes of water on the cloud. The Pryor Fire Department received the call at 10:45 a.m., and the Chouteau and Locust Grove Fire Departments were immediately called for mutual aid. All three fire departments arrived with tankers and pumpers ready to provide backup help. The safety manager of Pryor Chemical said no other facilities were impacted by the ammonia incident. Plant officials evacuated the front part of the property for safety reasons. Employees were taken out through a gate to a safe area. Other plants were notified of the incident as a precautionary measure. News of the accident spread quickly through the community, with the story taking on several versions. One text message circulating stated that plants at MidAmerica had been evacuated and people were being told to stay indoors. "The fire department never issued an evacuation order for anybody," said an official. Pryor Chemical, a fertilizer manufacturer, has been in business for several years at MidAmerica Industrial Park. Source: <http://pryordailytimes.com/local/x383283312/Ammonia-leak-contained-in-plant>
8. *June 24, Minnesota Public Radio* – (Minnesota) **State to ask 3M to pay for environmental damage.** The State of Minnesota will ask 3M to pay for environmental damage due to contamination from the company's operations in Cottage Grove. 3M manufactured chemicals known as PFCs, used in stain and fire-resistant materials, until 2002. The chemicals seeped from disposal sites into the Mississippi River. The state imposed fish-consumption advisories on the river as a result of the contamination. 3M has paid for cleanup, and for improvements to public and private water systems. But now, according to the Minnesota Pollution Control Agency, the company will be asked

to pay for damage to the state's natural resources.

Source: <http://minnesota.publicradio.org/display/web/2010/06/24/3m-pfc-pollution/>

9. *June 24, Palos Heights Regional* – (Illinois) **Tanker's caustic fumes evacuate Heights residents.** A tanker venting sodium hydroxide forced the evacuation of residents within an approximate half-mile of 75th Avenue and Route 83 June 18 in Palos Heights, Illinois. A police officer spotted fumes venting from the top of the eastbound tanker around 5 p.m. and pulled the truck over at Lake Katherine Drive. The officer then advised the driver to clear the immediate area. Palos Heights police utilized the reverse 911 code red system. Residents in Lake Katherine and east of 75th Avenue were evacuated from their homes for about three hours, the Palos Heights Fire Protection district chief said. The businesses at Southwick Commons were also evacuated as the wind was blowing to the east. "There were about six violent plumes as the truck vented," he said. The last venting occurred when the truck released what he called "a large amount of vapor product from the bottom of the truck." Crews from the Environmental Protection Agency (EPA), the Metropolitan Water Reclamation District, the Southwest Hazardous Materials Response Team and Palos Heights Fire Protection District, and police worked to secure the area and clean up the spilled chemical. The last venting from the bottom of the truck caused some of the sodium hydroxide to leak onto the grass, into the sewer and on a police officer and squad car. A dike was built around the sewer to prevent the chemical from further penetrating the system. A clean-up contractor vacuumed out the sewer. A small patch of grass caught on fire when the truck vented from the bottom. The police officer was not injured, and he and his squad car were decontaminated. Police re-opened College Drive around midnight, after the chemical was completely cleaned up. The truck driver was not cited with any violations.

Source: http://www.theregionalnews.com/atf.php?sid=19175¤t_edition=2010-06-24

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

Nuclear Reactors, Materials and Waste Sector

10. *June 24, Press of Atlantic City* – (New Jersey) **Errors in mock emergency at Salem nuclear plant force second test next month.** The State of New Jersey misidentified a town in a public announcement during a drill at the Salem nuclear power plant in Lower Alloways Creek Township, New Jersey, the state Office of Emergency Management said June 24. The mistake and a delay in getting instructions out to the public mean the state will have to conduct a second drill in July. The drill tested the state's response to a nuclear disaster May 18. In a mock public notice, the state misidentified a town that was subject to a fish advisory, officials said. The state also took 62 minutes to make all the necessary preparations to direct the public to evacuate, take shelter or consume potassium iodide pills in response to the nuclear accident. The Federal Emergency Management Agency said the directions should have been issued within 45 to 50 minutes. Everything else in the biannual drill went smoothly, state officials said.

Source: http://www.pressofatlanticcity.com/news/breaking/article_9bd33156-7fee-11df-ae4a-001cc4c03286.html

11. *June 24, WNDU 16 South Bend* – (Michigan) **Cook Nuclear Plant activates emergency response after feeling earthquake.** The 5.0 earthquake centered in Ottawa, Canada was felt by Michiana, Michigan — and by the Cook Nuclear Plant in Bridgman. According to reporters at WSJM, the quake sent the plant into emergency action. No alarms went off, but workers at the plant felt the tremors and decided it was better to be safe than sorry. They activated the lowest of the plant’s four emergency responses and the area was thoroughly inspected for damage. No damage was found. Source: <http://www.wndu.com/localnews/headlines/97110949.html>

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

Critical Manufacturing Sector

12. *June 25, Reliable Plant Magazine* – (New York) **OSHA cites Ford for unsafe overhead cranes at Buffalo Stamping Plant.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) has cited the Ford Motor Company’s Buffalo Stamping Plant in Hamburg, N.Y., with an alleged willful violation of safety standards for not repairing or removing unsafe overhead cranes from service. The citation follows an OSHA inspection opened in January 2010 in response to a complaint from workers at the plant. OSHA standards require that employers inspect cranes to identify unsafe conditions and remove the cranes from operation until the hazards are corrected. OSHA’s inspection found five instances where overhead cranes used to lift and set dyes or lift coils of steel were allowed to remain in service after defects were identified during inspections conducted in 2008, 2009 and 2010. The defects included worn brake drums, loose or sheared coupling bolts, and worn or damaged gears. “Management’s ongoing knowledge of and failure to correct these repeatedly recognized defects exposed workers to potential crushing injuries had one or more of these cranes failed,” said OSHA’s area director for western New York. “It should not take an OSHA inspection and enforcement action to prompt an employer to complete necessary repairs that should have been made months, even years, ago.” Source: <http://www.reliableplant.com/Read/25265/OSHA-Ford-unsafe-cranes>
13. *June 24, WEAU 13 Eau Claire* – (Wisconsin) **Fire at Altoona manufacturing plant.** An Altoona, Wisconsin factory had to be evacuated because of a fire Thursday night. Crews were called to Curt Manufacturing about 9 p.m. Employees said there was a fire in a dust collector in the building. Firefighters said the fire was contained to the dust collector. Employees said everyone got out safely. Investigators are trying to figure out what caused the fire. The plant had two fires in 2009, and one in May 2010. Source: <http://www.weau.com/news/headlines/97129294.html>
14. *June 24, WNDU 16 South Bend* – (Indiana) **Wednesday’s storm damages Warsaw Foundry, uproots trees.** Residents in Warsaw, Indiana said a storm June 23 sounded like a train ripping through town. Power lines were down, trees uprooted, cars crushed,

and buildings damaged. The Warsaw Foundry saw some of the worst damage in town. A resident said, “It ripped the whole roof off of that, sent it clear over the railroad tracks into these people’s back yard.” The foundry suffered a natural gas leak as well. The Warsaw Foundry was able to stay open for business June 23. The company said they hope to have their roof repaired by Monday.

Source: <http://www.wndu.com/hometop/headlines/97101124.html>

For another story, see item [25](#)

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

Defense Industrial Base Sector

15. *June 25, Fire Fighting News* – (Connecticut) **Firefighters keep flames from reaching chemicals.** A three-alarm fire on lower Chapel Street just north of New Haven Harbor in Connecticut Thursday damaged a large manufacturing plant filled with flammable and potentially toxic chemicals, but the mayor said the blaze was significant for what didn’t happen. “The story here is the dog that didn’t bark,” he said. “You didn’t have a fireball here. We didn’t have a (toxic) smoke plume.” That was in doubt for a time when fire started in the boiler room of the 41,900-square-foot industrial building and quickly spread toward the main, manufacturing section. The fire department was called at about 8:45 a.m. The building houses Swiss-based company Von Roll Isola and produces electrical insulation and has military contracts to produce insulation for Army helmets. Extremely flammable lacquers and solvents are used in part of the manufacturing process, he said, and were stored in a different part of the building. The department knew of the potentially explosive contents as they arrived. As part of incident planning, the fire service confers with manufacturers and asks them to provide inventories of hazardous materials contained inside. In addition to the possible explosion, if the chemical had ignited it would have sent a toxic plume of smoke through the neighborhood, creating larger concerns for firefighters and civilians. There were no injuries to workers or firefighters.

Source: <http://www.firefightingnews.com/article-us.cfm?articleID=80764>

16. *June 24, WAVY 10 Hampton Roads* – (National) **Bush conducts first missile launch.** The aircraft carrier USS George H.W. Bush (CVN 77) successfully fired two Evolved NATO Sea Sparrow missiles and two Rolling Airframe Missiles (RAM) for the first time, to conclude its first Combat Systems Ship’s Qualification Trials (CSSQT) Wednesday. CSSQT is part of the series of qualifications and certifications the aircraft carrier must undergo in preparation for her upcoming maiden deployment. According to the ship’s Combat Systems Officer, CSSQT is a combined effort between the Combat Systems, Operations and Weapons departments to test the aircraft carrier’s self-defense systems. “It’s an end-to-end testing of the Combat Systems Suite, to include tactics, techniques, and procedures,” he said. “It’s an operational verification of the ship’s warfighting and self-defense capabilities. Combat Systems with Operations department has worked around the clock for the last six months, grooming equipment and training for this exercise. More than 200 personnel have directly or indirectly

supported this evolution.”

Source: <http://www.wavy.com/dpp/military/USS-George-H-W-Bush-conducts-first-missile-launch>

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

Banking and Finance Sector

17. *June 25, MarketWatch* – (National) **Negotiators in Congress OK sweeping reform of big banks.** House and Senate lawmakers early June 25 approved the most significant increase in the regulation of U.S. banks since the Great Depression, placing new restrictions on the nation’s biggest lenders, reining in the Federal Reserve and crafting new consumer protections. It requires “too-big-to-fail” banks to install new capital and leverage limits, instructs the government to conduct unprecedented ongoing audits of the Fed’s lending programs, as well as a one-time audit of its emergency response programs. Also included in the sweeping package is a tough rule that would limit insured banks’ speculative proprietary trading activities. The controversial proposal would also force big banks to divest their major interests in hedge funds and private equity firms, allowing them to hold no more than 3 percent of a fund’s capital, though big banks could have as long as seven years to comply.

Source: <http://www.marketwatch.com/story/house-senate-panel-nears-sweeping-big-bank-reform-2010-06-25>

18. *June 25, CNN* – (California) **‘Geezer bandit’ wanted in string of bank robberies.** A Southern California bank robber dubbed the “geezer bandit” has struck again, possibly knocking off his 11th bank, the FBI said. The suspect held up a Bank of America branch in Temecula June 24. “During (the) robbery, the robber approached the victim teller and presented a demand note for cash,” a statement from the FBI said. “The robber carried a leather case which contained a small caliber pistol that he threatened to use, if the teller did not comply with his demands.” The FBI believes the suspect is responsible for robbing 10 banks in San Diego County and one in Riverside County. The “Geezer bandit” has carried a weapon in at least two of the robberies and should be considered dangerous, authorities said. The robber has been described as between 60- and 70-years-old. However, there has been some suggestion that he may be wearing a mask to conceal his real age and make him appear much older than he is.

Source: <http://edition.cnn.com/2010/CRIME/06/25/geezer.bandit/?fbid=9uAZ-CfXyu8>

19. *June 25, Bloomberg* – (International) **G-20 protesters expand rallies as Toronto braces for summit.** Protesters and community groups aim to intensify their demonstrations in Toronto June 25 as businesses in the downtown of Canada’s largest city start to close ahead of the weekend’s Group of 20 summit. “There’s going to be a rally, a march, a block party and a tent city that’s going to go overnight,” a spokesman for the Toronto Community Mobilization Network said in an interview. Toronto’s core is shutting down ahead of the arrival of world leaders, with at least 36 branches of banks including Toronto-Dominion Bank closed. A 12-block section of Toronto’s downtown is surrounded by concrete barriers and 10-foot high metal fencing, part of

the largest security operation ever in Canada with 20,000 police and security guards. Starting at 8 p.m. June 25, only people who work in the security zone or are accredited for the summit at the Metro Toronto Convention Centre will be allowed to pass the gates. Canada is spending as much as C\$1.2 billion (\$1.15 billion) for the meetings to host world leaders, including C\$930 million on security.

Source: <http://www.businessweek.com/news/2010-06-25/g-20-protesters-expand-rallies-as-toronto-braces-for-summit.html>

20. *June 24, Bank Systems and Technology* – (International) **Australian bank to use bank of New Zealand’s anti-card-skimming technology.** National Australia Bank has begun using card-fraud prevention technology developed by one of its subsidiary banks, Bank of New Zealand. The technology, called Liquid Encryption Numbers (LEN), is intended to prevent the skimming of cards, where information on magnetic stripes is captured by criminals without the customer’s knowledge, by attaching an illicit card reader to an ATM or using a pocket reader to scan a card en route to a cash register. LEN changes the magnetic stripe information every time a customer visits a bank ATM, so if a criminal captures the information and clones the card, he or she won’t be able to use it to commit fraud. LEN was invented by a fraud initiatives manager at Bank of New Zealand. Bank of New Zealand has been using LEN for two years and said its fraud numbers have decreased. According to ACI Worldwide, one in five consumers around the world was hit by debit or credit card fraud over the last five years.

Source: <http://www.banktech.com/payments-cards/showArticle.jhtml?articleID=225701311>

21. *June 24, Eweek* – (International) **Inside text message phishing attacks.** Not all phishing takes place online. Text-message-based phishing, called smishing, is still out there, and though on the decline, a report from security vendor Internet Identity (IID) shows it is still being used to target credit unions. In smishing, scammers use text messages to impersonate companies and lure victims into calling a fake interactive voice response (IVR) system designed to steal personal data like account credentials and Social Security numbers. “The most common text phishing is text-to-phone, where text messages are sent to potential victims with the goal of getting those victims to call a phone number provided in the message,” explained the CEO of IID. “When a victim calls the number, they are presented with an interactive voice response tree that often mimics the target institution’s own system. This system draws out and collects account access credentials from the victims.” Less common is text-to-Website, where the text message lures the victim to a traditional phishing Website, he added. According to the CEO, the attack patterns suggest there are no more than a few groups perpetrating text-phishing attacks as opposed to several dozen perpetrating other forms of phishing. IID reported the prevalence of the attack dropped 62 percent during the first quarter of 2010.

Source:

http://securitywatch.eweeek.com/phishing_and_fraud/inside_text_message_phishing_attacks.html

22. *June 23, Agence France-Presse* – (International) **Fake ATM dupes China bank customers.** Thieves in Beijing set up a fake ATM machine that recorded the bank details of unsuspecting users whose accounts were later robbed, in the first such scam discovered in China, state press said June 23. Having duped bank customers into revealing their account details, the thieves forged duplicate bank cards to drain their accounts, China Central Television said. The machine was bought from a legitimate manufacturer, but was not affiliated to any bank, it added. The ATM was placed on a busy corner in central Beijing and advertised that it could accept many major credit and bank cards, but all transactions resulted in an error message, the official China Daily reported. According to the paper, one man who used the machine was robbed of 5,000 yuan (\$735), while another person had his bank account “drained” of an unspecified amount. No arrests have yet been made.

Source:

<http://www.google.com/hostednews/afp/article/ALeqM5jG4j6DtXkofKOOcLmUAsOQ0tcWgg>

For another story, see item [61](#)

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

Transportation Sector

23. *June 25, The Washington Post* – (Maryland) **The heat is on Md. transit officials to improve MARC train safety.** On June 21, riders sweated through their clothes in the stalled cars of the Maryland Transit Administration’s (MTA) Maryland Area Regional Commuter (MARC) Train 538 for nearly two hours as temperatures inside climbed above 100 degrees. At the end of the ordeal, two people were taken to the hospital. For Maryland commuters, what happened to Train 538 near New Carrollton marked neither the first — nor the worst — such breakdown. Last summer, problems with aging MARC locomotives in dealing with high temperatures made similar delays a frequent occurrence. Ridership on the MARC rail system has grown rapidly in recent years, to 33,000 riders per day, but its infrastructure has failed to keep pace. The trains are owned by the state of Maryland but operated by contractors, and communication between train crews and the MTA can be poor. MTA, Amtrak and the Federal Railroad Administration are launching an investigation into the June 21 incident, but no official findings are anticipated for nearly 60 days — too late to have any impact on summer travel. Already, the MTA is taking simple steps to improve travel, with plans to “pair up” locomotives during peak hours for enhanced reliability in case of breakdown, and add cafe cars to supply water.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/06/24/AR2010062405499.html>

24. *June 24, Associated Press* – (New Mexico) **Train bridge on fire, cause unknown.** The second-highest bridge on the 64-mile Cumbres and Toltec Scenic Railroad line between New Mexico and Colorado is impassable after being damaged by fire. The railroad said the fire broke out Wednesday night on the Lobato trestle north of

Chama in northern New Mexico. The cause is not known. A New Mexico forestry spokesman said the state fire marshal's office is investigating. The railroad said it's unclear whether the main steel structure was damaged or whether the blaze was confined to the wooden ties and framing. The railroad is offering passengers the option of being bused to Antonito, Colorado, for a train trip to Osier, Colorado, and back. Source: <http://www.newswest9.com/Global/story.asp?S=12702995>

25. *June 24, Associated Press* – (National) **Boeing may recommend more 767 inspections.** Boeing said it is likely to recommend more inspections for some of its 767s after American Airlines found cracks where the engine attaches to the wing. Boeing is considering asking airlines to inspect the wings every 400 flights, a spokesman said Thursday. He said Boeing wants airlines to evaluate how the proposed change would affect their maintenance and flight operations. He said the new recommendation, called a service bulletin, is expected in mid-July. Currently the Federal Aviation Administration (FAA) requires inspections every 1,500 flights. But the cracks on at least two American jets were found after fewer flights. That raises the possibility that the wings are more susceptible to cracks than previously thought. American has already inspected all 56 of its affected planes. About 260 jets built before June 1997 are involved. Planes built after that had a different design that prevents the cracks, the spokesman said. Another 400 planes built before 1997 were retrofitted with a reinforced wing strut aimed at preventing the cracks. The extra inspections would only be mandatory if the FAA issues its own order. It has not decided whether to mandate the increased inspections and is waiting to see Boeing's service bulletin, an FAA spokesman said. Other operators of the affected jets include Delta Air Lines, United Airlines, Continental Airlines, and US Airways. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/06/24/AR2010062403183.html>

For more stories, see items [4](#), [9](#), and [68](#)

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

Postal and Shipping Sector

26. *June 25, Belleville News-Democrat* – (Illinois) **White powder closes Scott AFB building.** A building at Scott Air Force Base in Belleville, Illinois was briefly closed June 24 in response to a possible hazardous material scare. A secretary in building 1961, which houses part of U.S. Transportation Command, was opening mail when she found a white, powdery substance in one of the envelopes around 9 a.m., according to information provided by Scott Air Force Base. The letter was addressed to a senior leader who works in the building. Parts of the building were evacuated and the area was cordoned off. Hazardous-material and bioenvironmental technicians as well as fire and medical teams responded to the report of the substance. The powder was tested and found negative for biological or chemical material. The area was declared safe around 11 a.m. The substance will undergo additional testing, and the Office of Special Investigations will continue to investigate the incident.

Source: <http://www.military.com/news/article/white-powder-closes-scott-afb-building.html?ESRC=topstories.RSS>

27. *June 24, Associated Press* – (South Dakota) **Teens admit to mailbox bombs in Huron area.** Beadle County authorities said three teenagers have admitted to planting pipe bombs in mailboxes. Four mailboxes in the Huron, South Dakota area have been destroyed in the past month. No one has been hurt, but the explosions were powerful enough to be heard from several miles away. Authorities said they tracked down the suspects through tips. The teens might face charges.

Source: <http://www.kcautv.com/Global/story.asp?S=12704185>

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

Agriculture and Food Sector

28. *June 25, Food Safety News* – (International) **Brazilian beef products recalled for drug residues.** Sampco, Inc. of Chicago, Illinois is recalling approximately 61,000 pounds of cooked canned and frozen beef products that may contain the animal drug Ivermectin, the U.S. Department of Agriculture's (USDA's) Food Safety and Inspection Service (FSIS) announced June 24. Ivermectin is an antiparasitic used to deworm live animals. In May, FSIS discovered residues of Ivermectin above the U.S. Food and Drug Administration's (FDA's) tolerance level for beef muscle in products from Brazil, which sparked an 87,000 pound Class II recall, with low-health risk, for related beef products, also from Sampco. The agency believes the recently recalled product may have entered the country through a separate route of entry. The following products are subject to recall: 12 oz. cans of "Deltina Corned Beef With Juices" with the production code "100120" on the top of the can. These products were sent to a distribution center in Florida for retail sales; 12 oz. cans of "Hormel Corned Beef With Natural Juices" with the production code "100120" on the top of the can. These products were sent to distribution centers in Guam for retail sales; 35 lb. boxes of frozen "Seasoned Cooked Beef." These products were distributed to federal establishments for processing; and 35 lb. boxes of "Sampco Brand Frozen Cooked Beef, Salt Added." These products were distributed to federal establishments for processing. Each product package bears "BRASIL 337 S.I.F," as well as "Product of Brazil" or "Packed under Brazilian Government Inspection." The products subject to recall were produced in Brazil on January 20, 2010.

Source: <http://www.foodsafetynews.com/2010/06/brazilian-beef-products-recalled-for-drug-residues/>

29. *June 25, Atlanta Journal Constitution* – (Georgia) **Bomb threat suspect wants name changed to 'Mr. Lunatic'.** A Fulton County, Georgia judge set bond Friday for the Kennesaw man who allegedly told Atlanta police Thursday night that he had left an explosive device in a Kroger parking lot, forcing authorities to shut down Peachtree Road for several hours. But the magistrate denied a request by the defendant that his name be changed to "Mr. Lunatic." The 45-year-old was harged with making terroristic threats and causing a false public alarm for allegedly claiming — falsely — to have left

an explosive device in the Kroger parking lot the night of June 24. Police went to the shopping center near the Brookwood Interchange around 9 p.m. after receiving a report of a suspicious individual in sitting in the Kroger parking lot. “When the officer approached the male, he advised the officer he had a detonator,” a representative said. “The officer retreated, notified his supervisor and they called SWAT.” Peachtree Street in that area was then closed for about two hours while officers looked for a bomb. No explosives were found.

Source: <http://www.ajc.com/news/atlanta/police-identify-man-accused-557128.html>

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

Water Sector

30. *June 25, Water Technology Online* – (Mississippi) **Boil-water alert issued in Jackson, Miss.** The city of Jackson, Mississippi, is under a boil-water alert after a 54-inch water main malfunctioned Thursday, WAPT Jackson reported. The cap blew off of the water line and caused the O. B. Curtis Water Plant to shut down, resulting in a loss of system pressure, according to officials. Water service has been restored and testing is underway, the article stated. “We didn’t want to create a situation that would have people think that the sky is falling,” said the mayor. “We were losing pressure, but certainly at midnight, we didn’t know that we had a 54-inch, water-line break. In fact, we had to go find where the break was. It’s actually in an isolated area. We didn’t know exactly what was happening. We wanted to get information on what was happening before we actually issued any kind of notice.”

Source: http://watertechonline.com/news.asp?N_ID=74378

31. *June 24, Tampa Tribune* – (Florida) **Plant City’s sinkhole-threatened water tank back in service.** A 500,000-gallon water tank that was threatened by unstable soil, including a sinkhole, has been placed back in service. Earth Tech LLC of Land O’ Lakes shored up the soil around the elevated tank near Plant City Airport in Plant City, Florida. City officials worried that the tank was in danger of falling and had drained it until the soil was stabilized. The Plant City area was plagued with sinkholes after growers pumped millions of gallons of water in early January to protect their tender crops from the cold. Some homes were destroyed by the sinkholes, and lanes of several roads closed until they could be repaired. The mayor said the reopening of the water tank was welcome. The city has three other water tanks that were not impacted by unstable soil and remained in service. The city commissioner said the water tank placed back in service seems to be working fine.

Source: <http://www2.tbo.com/content/2010/jun/24/plant-citys-sinkhole-threatened-water-tank-back-se/news-breaking/>

32. *June 23, Kansas City Star* – (Missouri) **Sewer line breaks, spills raw sewage into Swope Park creek.** An estimated 81,000 gallons of raw sewage spilled into a creek in Swope Park before workers were able to fix a broken pipe, Kansas City, Missouri officials said Wednesday. After the sewer line break was discovered Tuesday, Kansas City water services workers replaced about 45 feet of the line. More extensive repairs

will be done, a press release said. The break in the 18-inch sewer pipe was south of the Swope Memorial Golf Course and near a picnic area located near Oldham Road and Oakwood Road. The creek leads to the Blue River. Workers posted signs to inform the public of the discharge. The city is working with the state to mitigate the impact of the spill.

Source: <http://www.kansascity.com/2010/06/23/2039406/sewer-line-breaks-spills-raw-sewage.html>

33. *June 22, UPI* – (Colorado) **Wastewater chemicals change gender of fish.** Scientists say chemical endocrines remaining in water after treatment at some U.S. wastewater plants can change the gender of fish. Researchers said male fish are still being feminized by chemicals, such as the pharmaceutical ethinylestradiol, passing through the Boulder, Colorado, Wastewater Treatment Plant and into Boulder Creek, though it is taking longer to happen since a plant upgrade to an activated sludge process. The scientists from the University of Colorado-Boulder said the chemicals are endocrine disrupters that mimic estrogen and can disrupt the endocrine (hormonal) system of both animals and humans.

Source: http://www.upi.com/Science_News/2010/06/22/Wastewater-chemicals-change-gender-of-fish/UPI-46141277239932/

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

Public Health and Healthcare Sector

34. *June 25, Belleville News-Democrat* – (Illinois) **Caustic chemical spilled in Memorial Hospital operating room.** Emergency personnel and members of the St. Clair County Hazardous Materials Team were called Thursday afternoon to Belleville Memorial Hospital in Belleville, Illinois, after a small amount of a caustic chemical was spilled in an operating room. Four employees who were exposed to the fumes were checked out for respiratory issues, a Memorial Hospital spokeswoman said. Four surgeries, including one open-heart surgery, were in progress in adjoining rooms during the spill and had to be allowed to continue, Belleville's fire chief said. Firefighters sealed the contaminated operating room and emptied the other operating rooms as the surgeries were completed. The fire chief said a man was splashed when a glass bottle of phenol shattered on the floor, and three nurses were exposed to the fumes. They were all treated at the hospital's emergency room. Phenol is a caustic substance used by doctors to cauterize wounds. "No one was burned by it," the hospital spokeswoman said. "It was spilled on the floor, but, if inhaled, it can cause some respiratory discomfort." The spill occurred about noon and emergency personnel, including members of the Belleville Fire Department, were working Thursday afternoon to clean up the operating room and remove the substance from the property, the spokeswoman said. All the operating rooms were expected to be back in use Friday, she said. Operating rooms on the other side of the hospital were not affected by the spill.

Source: <http://www.bnd.com/2010/06/25/1307021/caustic-chemical-spilled-at-memorial.html#ixzz0rsbZhvkr>

35. *June 25, Homeland Security Today* – (National) **VA key player in emergency ‘surge capacity’**. The House subcommittee on Oversight and Investigations evaluated the U.S .Department of Veterans Affairs’ (VA) role in emergency preparedness in a hearing June 23. The hearing assessed VA’s emergency preparedness posture, also known as the Fourth Mission, especially its role in preparing for and responding to large scale natural and man-made disasters as a backup to the Department of Defense (DoD) health care system. “While FEMA and the Department of Health and Human Services tend to take the lead role whenever an emergency occurs, one cannot deny the large importance of emergency preparedness at the VA,” a Tennessee Representative declared, noting the vast network of the VA healthcare system, which currently encompasses 153 hospitals and 788 community outpatient clinics. In his statement, the Assistant Secretary of Operations, Security and Preparedness at the US Department of Veterans Affairs assessed the VA’s emergency preparedness response since Katrina and affirmed the need for continuing “comprehensive assessment of all VA medical centers,” and providing “an internal VA patient-evacuation system that does not rely on outside resources.”
Source: <http://www.hstoday.us/content/view/13756/149/>
36. *June 22, Homeland Security Today* – (National) **New disaster toolkit assists special needs populations**. A new toolkit “meant to assist state and local public health agencies improve their emergency-preparedness activities” for special-needs populations has been released under a project funded by the Department of Health and Human Services Office of the Assistant Secretary for Preparedness and Response. Executed by the Center for Public Health Preparedness within RAND Health, the toolkit “distills the most relevant strategies, practices, and resources from a variety of sources.” The report of the program that developed the toolkit, Enhancing Public Health Emergency Preparedness for Special Needs Populations: A Toolkit for State and Local Planning and Response, stated that “experiences from recent emergencies, such as Hurricanes Katrina and Rita, have shown that current emergency preparedness plans are inadequate to address the unique issues of special needs populations.”
Source: <http://www.hstoday.us/content/view/13706/149/>

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

Government Facilities Sector

37. *June 25, Fox News* – (National) **AWOL Afghans found ... on Facebook**. At least 11 of the 17 members of the Afghan military who went AWOL from an Air Force base in Texas have turned up on Facebook. Some belong to the “Afghanistan Mujahideen” group, a page that features, among other content, videos from the American-born al Qaeda spokesman Azzam the American. According to a nationwide be-on-the-lookout (BOLO) bulletin that was sent by the North Texas Joint Terrorism Task force to law enforcement agencies across the country the week of June 14, the 17 Afghan deserters walked away from the Defense Language Institute at Lackland Air Force Base, where they had been studying English. The men have military identification that would give them access to secure U.S. military installations, the bulletin read. One week later, an

Immigration and Customs Enforcement source said that only two or three of the 17 Afghans remain at large. The source said investigators have been working with Canadian immigration records and now believe that many of the men are in Canada. A spokesman for Randolph Air Force Base in Texas said he was told that four of the men remain unaccounted for. Of the 13 who have been located, he said, six have pending refugee claims in Canada, two have permanent residency in Canada, four are in the process of being deported, and one is a conditional resident alien in the U.S.

Source: <http://www.foxnews.com/us/2010/06/25/exclusive-awol-afghans-found-on-facebook/>

38. *June 24, American Statesman* – (Texas) **Burnet County Courthouse briefly evacuated due to suspicious activity.** On June 24, the Burnet County Courthouse in Burnet, Texas was evacuated for about two hours in response to a suspicious activity investigation. About 9:50 a.m., the Burnet County Sheriff's Office was notified that an unidentified male was observed leaving two unattended suitcases in the vicinity of a bench located on the first floor of the courthouse. Upon locating the suitcases and consulting with the Austin Police Department Bomb Unit, the courthouse and surrounding buildings were evacuated until the arrival of the bomb unit. As the investigation progressed, the identity of the owner of the suitcases was determined. The man was questioned and released after the bomb unit determined that the contents of the suitcases were not hazardous. The courthouse and surrounding buildings were reopened at approximately 11:45 am. No charges are expected to be filed in this incident.

Source: http://www.statesman.com/blogs/content/shared-gen/blogs/austin/blotter/entries/2010/06/24/burnet_county_courthouse_brief.html

39. *June 24, Mayville Ledger Independent* – (Kentucky) **Lewis County Courthouse evacuated after bomb threat.** The Lewis County Courthouse in Vanceburg, Kentucky was evacuated June 24 after officials said a bomb threat was received. The Lewis County deputy said the call was received about 10:15 a.m. The caller said there were three bombs in the Vanceburg area but only mentioned the location of one, which he said was in the courthouse. The deputy clerk received the call then called the sheriff's office. A search was conducted by members of the sheriff's department and the Kentucky State Police. The call was cancelled soon after. The deputy said he believes the call was a hoax, but the sheriff's department intends to find the perpetrators. The deputy said the caller could be charged with wanton endangerment or terroristic threatening, possibly up to 75 counts, one count for each person who was in the courthouse at the time the threat was received.

Source: http://www.maysville-online.com/news/local/article_90054d06-800b-11df-b084-001cc4c002e0.html

40. *June 23, Federal Computer Week* – (National) **Just how continuous should continuous security monitoring be?** It's common knowledge that governmental organizations should regularly assess their security readiness. But how often should they scan their security assets and system configurations? The National Institute of Standards and Technology's Special Publication 800-53 Revision 2 describes periodic

assessments of risk, while Revision 3 refers to monitoring risk on an ongoing basis. Control 10 of the Consensus Audit Guidelines (CAG) deals with “continuous vulnerability assessment and remediation.” It has been up to agencies to determine what that means in terms of frequency. Just how continuous should continuous security monitoring be? Twenty critical security controls that organization should be focusing on “Back when (the Federal Information Security Management Act) started and concentrated on process and compliance snapshots, it was not unusual to do scans two or three times a year,” said the State Department’s chief information security officer. However, given the current security environment, such monitoring needs to occur more frequently.

Source: <http://few.com/articles/2010/06/28/feat-cybersecurity-measuring-continuous-box.aspx>

For another story, see item [26](#)

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

Emergency Services Sector

41. *June 24, Associated Press* – (Texas) **Blast at training center maims West Texas officer.** A West Texas bomb technician has been injured critically when a bomb he was dismantling exploded at a police training center. A Midland police sergeant was injured about 11 a.m. June 24 at the Midland police training center. A Training Division lieutenant tells the Midland Reporter-Telegram that the sergeant may have lost his left hand and suffered injuries to his left arm. He was transferred to University Medical Center in Lubbock. The device exploded while he was removing an aluminum casing from the device to prepare it for a training exercise where officers neutralize oil field explosives. The U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives and Midland police will investigate.

Source: <http://www.chron.com/disp/story.mpl/ap/tx/7078902.html>

42. *June 23, Yuma Sun* – (Arizona) **Woman escapes in U.S. Marshals’ car.** A woman is on the run after escaping in a U.S. Marshals’ car Wednesday near Avenue C and 3rd Place in Yuma, Arizona. The woman had reportedly been handcuffed and placed in the back of an undercover Marshals’ vehicle after being arrested for an outstanding warrant. “She stole their car,” said a Yuma County Sheriff’s Office (YCSO) spokesman. “She was handcuffed, but apparently she was able to get them off or in front of her, and climbed over the seat and took off in their car when they were not paying attention. This was an undercover car ... and it didn’t have [a cage separating the front and back seats].” The suspect then crashed the car into a fence in the 300 block of Ruby Avenue, where she fled on foot, police said. In the process, a federal agent was injured and later treated at Yuma Regional Medical Center for non-life-threatening injuries before being released. YCSO, the U.S. Marshals Service, Yuma Police Department, U.S. Border Patrol, and FBI agents established a perimeter and searched door to door trying to locate the suspect. She is wanted for the alleged escape, felony

flight, vehicle theft and for allegedly committing aggravated assault on a federal agent.
Source: <http://www.yumasun.com/news/car-61950-herrera-vehicle.html>

43. *June 23, CBS News* – (New Jersey) **FBI agent loses rifle, bulletproof vest.** CBS News has learned a FBI agent's automatic rifle and bulletproof vest were stolen from his vehicle in New Jersey while he was off duty June 19. The high caliber M4 rifle, a military version of the AR-15 rifle, fires a succession of three rounds with one pull of the trigger. The FBI's New Jersey office is currently searching for the weapon. "It makes our urgency even greater because the weapon is in the hands of a criminal," said a FBI spokesman in Newark, New Jersey Agents are sometimes authorized to have weapons in their car, he said. He would not elaborate on the security procedures involved. "As long as those protocols are followed then the FBI is permitted to store weapons in the vehicle," the FBI spokesman said. Agents are working around the clock to locate the stolen weapon and vest, he said. The spokesman refused to comment on what penalties FBI agents face when their weapons are lost.

Source: http://www.cbsnews.com/8301-31727_162-20008645-10391695.html

44. *June 23, Government Technology* – (Oregon) **Amateur radio operators aid government communications during emergencies.** Amateur radio operators, who use various types of radio communications equipment for nonprofit purposes, can provide a valuable resource to state and local governments during disasters. In Oregon, about 1,800 Radio Amateur Civil Emergency Service (RACES) volunteers are authorized to work in state and county emergency operations centers (EOCs) facilitating communication during disasters. For example, during the Great Coastal Gale of 2007 that knocked out communications to Columbia, Clatsop and Tillamook counties, ham radio operators used a radio-frequency messaging system called Winlink to transmit requests for assistance to the state's Office of Emergency Management (OEM). Following the storm, Oregon's governor funded improvements to the state's amateur radio infrastructure with a \$250,000 grant for Winlink systems in each of the state's 36 county-level EOCs. Amateur radio operators can play a variety of roles that allow public safety officials to maximize their resources, including facilitating communications; providing emergency managers with on-scene situational awareness; and helping manage large-scale events, such as state fairs and marathons. Earlier this year as blizzards blanketed Delaware, RACES members manned ham radio stations at the Sussex County EOC, and others drove around the county's 958 square miles reporting what they were seeing and confirming reports from the National Weather Service.

Source: <http://www.govtech.com/gt/articles/765536>

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

Information Technology Sector

45. *June 25, SC Magazine* – (International) **Researcher demonstrates Twitter XSS vulnerability.** A Twitter user has demonstrated a cross-site scripting (XSS) vulnerability on the microblogging platform that could allow an attacker to take over

users' accounts or spread malware. An Indonesian security researcher, using the alias "H4x0r-x0x" and Twitter handle "Own3d_5ys," discovered the vulnerability and demonstrated the bug using his own Twitter account. In addition, the researcher June 21 announced details about the flaw on his blog. The vulnerability affects the "application name" field on Twitter's application registration page, used by developers when setting up a new Twitter application. The flaw appears to be the result of a lack of input validation of the "application name field" when accepting new requests for Twitter applications, a partner at Praetorian Security Group told SCMagazineUS.com June 24. The flaw could be exploited by cybercriminals to insert malicious JavaScript code into a Twitter page. Visiting the researcher's Twitter account causes a pair of XSS alert boxes, followed by a user's browser being manipulated. The demonstration of the flaw also causes an animation from the film "The Matrix" to appear, followed by messages from the researcher, one of which states, "My Twitter Owned By : H4x0r-x0x.."

Source: <http://www.scmagazineuk.com/researcher-demonstrates-twitter-xss-vulnerability/article/173207/>

46. *June 25, The H Security* – (International) **Google uses remote delete to remove Android apps from smartphones.** Google has, for the first time, used the "Remote Application Removal" security feature implemented in Android to remove apps from users' smartphones. The two applications in question were created by TippingPoint security researchers who had deployed the apps to demonstrate how easy it is to inject malicious applications into Android smartphones and jailbroken iPhones. Although the researchers had removed the applications from the Android Market, some users still had the apps installed on their phones, prompting Google to delete them remotely. In such cases, users are notified that the deletion will occur. Google points out that the removed applications did not cause any damage, having been designed to show how easy it was to infect smartphones rather than to cause any malicious infection. Other mobile-device vendors also reserve the option for remote deletion and some have even exercised this option. In mid 2009, Amazon deleted the Kindle eBooks "1984" and "Animal Farm" by George Orwell, because the vendor in question was not licensed to distribute them. After a flurry of protests, Amazon promised that it would avoid such deletions in the future. Apple is also capable of remote deletion of installed applications from iPhones, but has not made use of this option so far. Originally, Google developed the remote-deletion feature to prevent the spreading of real malware and protect users. The vendor hopes that the option will never be needed on a large scale.

Source: <http://www.h-online.com/security/news/item/Google-uses-remote-delete-to-remove-Android-apps-from-smartphones-1029188.html>

47. *June 25, The Register* – (International) **Spanish firm raided in logic-bomb backdoor probe.** Three managers at an unnamed Spanish software developer have been arrested over allegations they planted "logic bombs" in software that meant clients were obliged to pay for disruptive repairs and extended maintenance contracts. The Guardia Civil said that more than 1,000 clients of the Andalusia-based developer have been affected by the scam since 1998. The unnamed firm sold marketed custom software to small- and medium-sized businesses with built-in errors such that it was guaranteed to fail at a

predetermined date. These errors would “paralyze the normal functioning of businesses” and oblige customers to contact their supplier, who would hit them for repair fees and extended support. In the course of making repairs, the developer allegedly programmed systems to fail again at a future date. An anonymous Web-based tip-off led to a Guardia Civil investigation and a subsequent raid on the firm’s premises, where computer equipment and records were seized for analysis. The investigation — codenamed Operation Cordoba — is being led by the Guardia Civil’s hi-tech division in cooperation with local police in Cordoba, Spanish daily El Pais adds. Source: http://www.theregister.co.uk/2010/06/25/spanish_logic_bomb_probe/

48. *June 25, The Washington Post* – (National) **Twitter settles with FTC over hacking breach.** Twitter has settled charges brought by the Federal Trade Commission (FTC) that it deceived consumers by allowing hackers to obtain administrative control over the popular social-networking service because of loose security. The FTC said June 24 that Twitter allowed hackers in 2009 to view private “tweets” — micro-blogs of up to 140 characters — and to send phony messages purportedly from the accounts of (the President) and Fox News, among others. Under the settlement, Twitter will set up a security program to be assessed by a third party and will be prohibited from “misleading consumers about the extent to which it ... protects ... nonpublic consumer information,” the FTC said. No damages were sought. In a statement, the Twitter general counsel said that relatively few users were affected by the breach, and that the incidents occurred when the company had 50 employees and was grappling with explosive growth. The company said that it has since worked on security measures, and that no other complaints have been brought regarding privacy or security lapses. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/06/24/AR2010062406473.html>
49. *June 24, Adobe* – (International) **Pre-Notification: Quarterly security updates for Adobe Reader and Acrobat.** A security advisory has been posted in regards to the upcoming Adobe Reader and Acrobat updates scheduled for June 29. The updates will address critical security issues in the products, including CVE-2010-1297 referenced in Security Advisory APSA10-01. These security updates will be made available for Windows, Macintosh and UNIX. Note that the June 29 updates represent an accelerated release of the next quarterly security update originally scheduled for July 13. With this accelerated schedule, Adobe will not release additional updates for Adobe Reader and Acrobat on July 13. Source: <http://blogs.adobe.com/psirt/2010/06/pre-notification - quarterly s 3.html>
50. *June 24, DarkReading* – (International) **Kraken botnet making a resurgence, researcher says.** The Kraken botnet — one of the Internet’s largest and most difficult to detect in 2008 — is rearing its ugly head again. In fact, the old security nemesis — which was reported dismantled last year — has compromised more than 318,000 systems, nearly half of the 650,000-node size it achieved at its peak in 2008, according to a research scientist at the Georgia Tech Information Security Center (GTISC), a leading authority on botnet research. So far, the resurrected Kraken is primarily a spam distributor, focusing most of its output on ads for male enhancement and erectile

dysfunction. The botnet's performance is prodigious: a single node with a DSL-speed connection was detected sending more than 600,000 spam messages in a 24-hour period. Many popular antivirus tools do not detect Kraken. A scan by VirusTotal indicates that none of the top three antivirus tools — Symantec, McAfee, and Trend Micro — can detect current Kraken samples, he reports. The resurrected Kraken is usually installed by another botnet, using botnet malware such as Butterfly, the researcher reports. It is not clear whether Kraken installation is handled by the same criminal group as Kraken operations, but it may be an example of specialized criminal groups working together, he suggests. Kraken's reappearance may indicate a broader trend toward the re-use of code.

Source:

http://www.darkreading.com/vulnerability_management/security/antivirus/showArticle.jhtml?articleID=225701438&subSection=Antivirus

51. *June 24, DarkReading* – (Unknown Geographic Scope) **iPads susceptible to iPhone malware, researchers say.** PandaLabs, Panda Security's antimalware laboratory, has revealed that malware designed to infect iPhones can also compromise the popular iPad, as demonstrated in a video on the PandaLabs blog. "This doesn't mean we're about to face an avalanche of infections. We have always stated that as Apple increases its market share, cyber-crooks will begin to show more interest in targeting the platform," said the technical director of PandaLabs. "However, we are certainly beginning to see more proofs of concept, and so advise all Mac users to follow the manufacturer's recommendations to maximize security on their operating systems." Despite the fact that Apple has made it impossible to install peripherals and software outside of those found in its own App Store, cyber-criminals have found a way to infect jailbroken iPad devices with malware. All malware designed for iPhones, such as the iPhone/EEKI.A worm that PandaLabs warned about last year, will have the same ability to infect and spread to iPad devices due to the iPad and the iPhone sharing the same operating system, known as iOS. Apple released iOS 4, the new version of its operating system, June 21. The iPhone/EEKI.A worm infected jailbroken iPhones. Jailbreaking refers to the process by which criminals tamper with iPhones in order to install applications that are not available in the official Apple App Store. In addition to the iPad, malware designed for the iPhone can also infect the iPad touch.

Source:

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=225701444&subSection=Vulnerabilities+and+threats>

52. *June 24, DarkReading* – (International) **ATT iPad breaches are about app security, not mobile devices, experts say.** The recent breaches of Apple iPad customer data at AT&T have drawn attention to security issues in both the mobile device and service provider spaces. But after analyzing the leaks, analysts said the lessons to be learned are not related to mobile or service vulnerabilities — they are lessons in the links between Web applications and back-end databases. "Mobile computing is no longer about mobile computing — it's really all about the Web," said the chief marketing officer for Web app security company Cenzic. "Most people don't realize that — even most telecom companies don't realize it — so they're focusing on the hardware piece.

But if you think about the end-to-end cycle of a mobile computing service — from acquisition to processing orders to customer service — it’s all on the Web.” Earlier this month, AT&T and its partner, Apple, found chinks in their Web application security armor when more than 100,000 iPad-user accounts were exposed due to a business logic flaw in a public AT&T Web application. Apple suffered a second privacy breach when users reported accessing other customers’ private information while preordering the latest iPhone through AT&T’s Web site. AT&T and Apple claimed they could not replicate the problem, but security experts, such as a researcher of WhiteHat Security, claimed the issues sounded suspiciously like session exhaustion, a behavioral anomaly that occurs when an application is overloaded and begins to run out of session IDs. Observers said both incidents likely involved poorly deployed Web applications that put sensitive back-end data at risk, giving nonauthorized users access to private database information.

Source: http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=225701411

53. *June 24, Help Net Security* – (International) **Phishing requires more effort than one might think.** When it comes to setting up phishing pages, there are some phishers that make the extra effort. Take those behind the fake Orkut log-in pages, for example. Symantec has been following their work, and noticed that phishers make the same changes to the Web sites that the original site makes - namely, the logo that changes on special occasions such as Earth Day, Mother’s Day, and others: Google had actually a pretty good idea with this logo-changing practice: not only does it make the services look more friendly and reminds the users that the sites are constantly monitored and updated, but it also makes “lazy” phishers fail.

Source: <http://www.net-security.org/secworld.php?id=9472>

54. *June 24, PCINews* – (International) **Amazon spam spreads Trojans.** A new wave of malware distributing phony Amazon e-mails is flooding users’ mailboxes. The spam messages are quite real-looking and, thus, can easily deceive recipients to follow the provided malicious links. The e-mails are hand-crafted and look so identical to those Amazon sends that many users have become easy prey of the crooks. The fake Amazon e-mail and the real one are almost identical. The differences between the two e-mails are few but vital: The real Amazon e-mail is addressed to the user by name, not by e-mail address. A spammer will not know a Amazon user’s name; the real e-mail shows the user’s billing address, the fake - not; finally, if a user place the mouse pointer over any link in the spam message, it will show that the links lead only to one single place - a Korean Web site Booksalon(dot)kr. There the Trojan lies and waits.

Source: <http://www.pc1news.com/news/1483/amazon-spam-spreads-trojans.html>

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>

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

Communications Sector

55. *June 25, PC World* – (National) **Apple responds to iPhone 4 antenna problem.** Since iPhone 4 smartphones reached the market June 22, several users reported poor reception issues with the device when holding the phone by its metal sides in two opposite places. The metal bands surrounding the sides of the iPhone 4 also act as antennas for the device, and the signal-drop problem seems to appear when a user touches both of the black lines on the phone’s metal sides towards the bottom, according to reports. An Apple statement recommends that if users are experiencing problems with the iPhone 4, they should “avoid gripping it in the lower left corner in a way that covers both sides of the black strip in the metal band, or simply use one of many available cases.”

Source:

http://www.pcworld.com/article/199853/apple_responds_to_iphone_4_antenna_problem.html?tk=hp_pop

56. *June 24, The Register* – (International) **VeriSign SSL certs open to tampering, competitor warns.** VeriSign and one of its partners have come under fire for publicly exposing Web pages used to process customer-security certificates, a practice a competitor claims puts some of the biggest names on the Web at risk of serious targeted attacks. According to the CEO of the Internet-security firm Comodo, publicly accessible pages needlessly disclose sensitive internal information about VeriSign customers; Bank of America and the Commonwealth of Massachusetts are two examples. By exposing the e-mail address of the organizations’ security-certificate managers, and providing a comprehensive list of Web addresses that use secure-sockets-layer protection, VeriSign puts them at risk of targeted phishing attacks, he said. The CEO noted that one page provided by VeriSign partner Getronics.nl of the Netherlands allows anyone in the world to search its database and pull up a wealth of information about the digital certificates of not only Bank of America but plenty of other companies, including VeriSign itself. The interface also points to dynamically generated pages, which provide buttons for revoking, renewing, and replacing the digital certificate.

Source: http://www.theregister.co.uk/2010/06/24/verisign_comodo_ssl_flap/

For another story, see item [44](#)

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

Commercial Facilities Sector

57. *June 25, Southeast Missourian* – (Missouri) **Cape man arrested for making bomb threats.** Cape Girardeau, Missouri police June 24 arrested a local man who they say made bomb threats against West Park Mall in Cape Girardeau, and the Walmart in Jackson, Missouri. A lieutenant of the Jackson Police Department said the store was cleared just after 4 p.m. While they didn't think there was any real danger, he said police took precautions. Walmart management made the decision to evacuate the store, he added, and police assisted. By 4:30 p.m., business was back to normal at the Jackson store. A spokesman for the Cape Girardeau Police Department said no bomb was found at the mall.
Source: <http://www.semissourian.com/story/1645143.html>
58. *June 25, WTMJ 4 Milwaukee & Milwaukee Journal Sentinel* – (Wisconsin) **1 Dead in wall collapse at O'Donnell Park.** Structural engineers from the City of Milwaukee, Milwaukee County and the State of Wisconsin will return to the collapsed parking garage early June 25 at O'Donnell Park. They will try to determine why a portion of the garage on Lincoln Memorial Drive near the Summerfest grounds collapsed, killing a 15-year-old boy and injuring two others. A spokesperson for Froedtert Hospital said that a female victim is in satisfactory condition, while a public relations official for Children's Hospital said that it took in one patient in the case who was treated and released. The sheriff's department said they were notified around 4 p.m. June 24 that a 30-foot slab of the structure collapsed. The parking structure remains shut down for the time being, but Lincoln Memorial Drive has been re-opened. Witnesses who saw the concrete fall said it appears that nothing caused it to fall, it just fell. After the collapse, crews quickly shut down parts of Lincoln Memorial Drive and put up a tarp.
Source: http://www.msnbc.msn.com/id/37910350/ns/local_news-milwaukee_wi/
59. *June 25, Associated Press* – (Washington) **Seattle Westin Hotel evacuated for small fire.** Several hundred guests at the downtown Seattle Westin Hotel were evacuated late June 24 while firefighters responded to a smoky fire on the fifth floor of the 47-story tower. KOMO-TV reports lint in a ventilation system caught fire. Firefighters quickly put it out and aired out the building so guests were back in their rooms by midnight.
Source:
http://seattletimes.nwsources.com/html/localnews/2012205743_apwaseattlewestinfire.html
60. *June 24, Winston-Salem Journal Reporter* – (North Carolina) **Gas-line leak forces evacuation of shopping center.** Authorities evacuated Shattalon Station shopping center in Winston-Salem, North Carolina June 24 after a construction crew broke a natural-gas line off Shattalon Drive near its intersection with Murray Road. No one was injured. The gas line was broken shortly after 2:45 p.m. as a crew with Yates Construction Co. was working on a widening project on Shattalon Drive, said the battalion chief of the Winston-Salem Fire Department. Police then evacuated the shopping center including a Food Lion store. Employees of Piedmont Natural Gas Co. worked to repair the gas line shortly after 3:30 p.m. Authorities then allowed

employees and customers to return to the shopping center.

Source: <http://www2.journalnow.com/content/2010/jun/24/gas-line-leak-forces-evacuation-shopping-center/>

61. *June 24, Toronto Sun* – (International) **Man arrested near G20 security site.** A 53-year-old Toronto man is under arrest after a G-20 Summit bike patrol found a cache of weapons, including a crossbow, in a car that was pulled over June 24. The car was stopped near the secure zone of the Group of Twenty Finance Ministers and Central Bank Governors summit in Ontario, Canada. Officers found three arrows, containers of gas, a slingshot, chainsaw, fire axe, saws, a tire iron, and other items in the vehicle. The accused also had a large piece of plywood that police suspect was for use in scaling G-20 security fences, officers said. The suspect, whose identity wasn't released by police, was driving an older model Hyundai Elantra that looked suspicious, police said. The suspect was stopped near the Novotel Hotel, where employees are on strike. Late June 24, police wearing rubber gloves were searching the vehicle, which had Ontario plates. The old car, which had a hand-made roof rack, was cordoned off with police tape. Officers weren't sure if they were going to call a bomb squad to examine the vehicle. Police from a hazardous-material unit were called to examine a second area that was roped off because of a possible gasoline spill. The suspect is expected to appear for a bail hearing June 25. The investigation is continuing.

Source: <http://www.torontosun.com/news/g20/2010/06/24/14501761.html>

62. *June 24, Baltimore Sun* – (Delaware) **Electrical room fire evacuates condos in Bethany Beach.** An electrical fire June 24 forced an evacuation of the Sea Colony high-rise complex in Bethany Beach, Delaware. A power surge caused a small fire inside an electrical room in one of the buildings, causing the evacuation at about 4 p.m., said a spokesman with the Bethany Beach Fire Company. The surge was caused by a downed wire. Smoke from the fire filled the complex, located at the Coastal Highway and Pennsylvania Avenue split, but the fire was contained. Residents were able to return after 35 firefighters secured to complex, and power was restored.

Source: http://articles.baltimoresun.com/2010-06-24/news/bs-md-bethany-electrical-fire-20100624_1_evacuation-electrical-room-fire

63. *June 24, DNAinfo.com* – (New York) **Upper East Side blaze evacuates building, sends two elderly residents to the hospital.** Two elderly people were rushed to the hospital and residents evacuated after a fire broke out in an Upper East Side apartment building in Manhattan June 24. Two senior citizens were found on the top floor of 200 East 71 Street after the fire department responded to the scene about 5:30 p.m., the Fire Department City of New York (FDNY) said. An elderly man was found inside one apartment and an elderly woman was in the hallway, a fireman on the scene said. Both were treated for smoke inhalation and are in stable condition at New York Hospital, a FDNY spokesperson said.

Source: <http://www.dnainfo.com/20100624/upper-east-side/upper-east-side-blaze-evacuates-building-sends-two-elderly-residents-hospital>

For more stories, see items [3](#) and [19](#)

National Monuments and Icons Sector

64. *June 25, Spokane Spokesman-Review* – (Idaho) **Dog killed by poisoned sausage on trail.** Idaho wildlife officials are asking for help in finding the person who placed poisonous sausage along a hiking trail north of Clark Fork in Idaho. One dog was killed and three others were sickened after they ate the tainted meat while their owners hiked along the trail. During the week of June 14, results from a test confirmed that the sausage, which was eaten by the dogs in April, was laced with Carbaryl, an insecticide that is illegal to use except to kill insects, said a senior conservation officer for the state Department of Fish and Game.
Source: <http://www.spokesman.com/stories/2010/jun/25/dog-killed-by-poisoned-sausage-on-trail/>
65. *June 25, The Denver Post* – (Colorado; New Mexico) **Wildfires flaring up across Colorado.** Fires were reported June 24 across Colorado, including in Elbert County, Grand County and Rocky Mountain National Park. The fires have burned more than 800 acres and have resulted in firefighting expenses of more than \$1 million. South of the border in New Mexico, the second-highest bridge on the Cumbres and Toltec Scenic Railroad was badly damaged by fire, disrupting service on the popular tourist attraction. The National Park Service June 24 requested four air tankers and six to eight smoke jumpers for a 3- to 5-acre fire burning in Rocky Mountain National Park.
Source: http://www.denverpost.com/news/ci_15372451
66. *June 24, Mid-Columbia Tri-City Herald* – (Washington) **White Bluffs slide seen at Hanford Reach.** A section of the White Bluffs across the river from Hanford, Washington's former F Reactor, slumped off the hillside the morning of June 23, a Hanford worker reported. He described the size of the landslide as about equal to the 2008 landslide of the clay bluff south of Ringold, if not larger, said a Washington Closure Hanford spokesman. Hours later, workers at the former nuclear power plant could still see dust rising from the slide area on the east side of the Columbia River on the Hanford Reach National Monument. Some of the slides that have collapsed sections of cliffs along the Columbia River have been blamed on seepage from irrigation water. This slide was on the national monument where there is no irrigation. However, there is a water wasteway that flows into the Columbia River farther north.
Source: <http://www.tri-cityherald.com/2010/06/24/1067542/white-bluffs-slide-seen-at-hanford.html>
67. *June 24, Associated Press* – (California) **Wildfire burning in mountains northeast of Los Angeles.** Firefighters are battling a 10-acre wildfire off a mountain road in the Angeles National Forest. A national forest spokesman said the blaze was reported shortly after noon June 24 and began as a series of spot fires off Highway 2 northeast of Wrightwood, California. A section of the road has been closed, but no evacuations have been called and no homes are threatened. Winds are light. About 120 firefighters from

several agencies are on the scene. The fire is in western San Bernardino County about 50 miles northeast of downtown Los Angeles.

Source: http://www.mercurynews.com/breaking-news/ci_15369139?nclick_check=1

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

Dams Sector

68. *June 25, Seacoastonline.com* – (New Hampshire) **Taylor River bridge and dam to be replaced.** The State of New Hampshire will replace the Interstate 95 bridge over the Taylor River and the Taylor River Dam, following a meeting held by the New Hampshire Department of Transportation June 21. The decision was based on a feasibility study which reviewed options for the two structures, including replacing the bridge and removing the dam, or doing nothing at all. The cost for the project to be completed will be about \$8,742,000. Though a decision has been made, obtaining the permit to rebuild the structures will take time. Mitigation must take place to reduce the build up of sediment. Water quality is also an issue that must be addressed. According to the study, top issues that must be addressed include the salinity level, dissolved oxygen levels, nutrients and plants in the water. The next steps in the process include: securing the necessary permits; addressing the water issues; having another public meeting to gain more comments, concerns and ideas from residents of Hampton and Hampton Falls; completing the final design of the structures by 2011; and beginning construction of the structures by 2013.

Source: <http://www.seacoastonline.com/articles/20100625-NEWS-6250325>

69. *June 24, U.S. Army* – (Louisiana) **Guard building coastal barriers to keep out oil.** Construction of 8.5 miles of wall barriers by the Louisiana National Guard's 225th Engineer Brigade continues in six areas along the coast of Cameron Parish in an effort to keep oil-tainted water from moving inland. Guard members assigned to engineer battalions from the 527th headquartered in Ruston, 528th headquartered in Monroe, and 769th headquartered in Baton Rouge, are working together to assemble and fill the barriers that will stretch along Highway 82, one of the parish's main highways. Though the oil is not currently coming on shore, it is important to build the wall now in order to protect more than 4,000 acres of marsh if the oil moves westward, aid the commander of the 928th Sapper Company, 769th, and one of the project managers. More than 150 soldiers are working on the month-long project. Even though many of the same Guardsmen helped build a similar barrier wall last month in Port Fourchon, the approach to building this barrier had to be altered to deal with the different terrain. The barrier is made up of a multi-cellular wall systems manufactured from welded, coated steel wire mesh and linked with vertical coil joints. Once erected, the units are filled with sand.

Source: <http://www.army.mil/-news/2010/06/24/41381-guard-building-coastal-barriers-to-keep-out-oil/>

70. *June 24, Fort Myers New-Press* – (Florida) **Water monitoring device missing from North Fort Myers dam.** Lee County, Florida, sheriff's deputies are searching for a

county water-monitoring device from a dam on Powell Creek in North Fort Myers. According to a sheriff's report, a Lee County engineer called deputies when he found the device missing. He said the theft occurred in the last three weeks. The device was removed and the only thing left was the lock that held the device to the dam, according to the report. The dam is located at Barbie Lane and the Del Prado extension.

Source: <http://www.news-press.com/article/20100624/NEWS0111/100624022/1075/Water-monitoring-device-missing-from-North-Fort-Myers-dam>

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

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact Information

Content and Suggestions:

Send mail to 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.