



Homeland Security

Daily Open Source Infrastructure Report for 1 July 2011

Top Stories

- The Los Angeles Times reports a Nigerian stowaway who flew from New York to Los Angeles, with an expired boarding pass in someone else's name was carrying at least 10 different boarding passes. (See item [20](#))
- Security researchers said a new and improved botnet that has infected more than 4 million PCs is "practically indestructible", according to Computerworld. (See item [46](#))

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: LOW, Cyber: LOW

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

1. *June 29, Washington Department of Ecology* – (Washington) **Boeing fined \$102,000 for Duwamish fuel spill.** The Washington Department of Ecology (WDOE) has fined The Boeing Company \$102,000 for spilling an estimated 300 gallons of jet fuel into the Duwamish Waterway in Seattle, Washington, in 2010. The spill occurred May 28, 2010, at a Boeing fuel terminal in south Seattle near the waterway. A tank truck was delivering jet fuel to an aboveground storage tank at the terminal. An operator heard and smelled leaking fuel and immediately stopped the delivery. The WDOE matched

oil samples from the river and from the Boeing facility to identify the May 28 incident as the source of the oil seen May 29 on the waterway. Besides the penalty, ecology also billed Boeing \$5,500 to recover the state's costs for conducting the spill cleanup and investigation.

Source: <http://www.ecy.wa.gov/news/2011/180.html>

2. *June 29, KMBC 9 Kansas City* – (Missouri) **KCP&L's Iatan power plant partially evacuated.** Kansas City Power and Light's (KCP&L) Iatan Power Plant was partially evacuated June 29 because of flooding. KCP&L confirmed the evacuation. The coal plant sits on the bottom land near the flooded Missouri River. It continued to operate. A spokesman reported floodwaters were sweeping into the plant property, its access roads, and employee parking lots. Utility officials said they are using "an abundance of caution" in pulling nonessential employees out of the power plant. A spokesman stressed the plant's operations were not affected. He said they have plenty of coal and other supplies on site should floodwaters cut off the main rail line into the plant. The spokesman said, if needed, the utility has a plan to bring workers to the plant by boat. He reported that the floodwaters would have to rise 3 feet to jeopardize the plant's operation. The Farley Bridge near Iatan caused concern, though, because it is used by the plant's railroad line to carry coal. Workers had to dislodge debris that collected under the bridge so the water wouldn't dam up. Many roads in the area were closed and officials in Weston were preparing for the water to come their way. A Weston Road district officials said \$150 fines would be issued to anyone who drove past a "road closed" sign.

Source: <http://www.kmbc.com/r/28396205/detail.html>

3. *June 26, KBAK 29 & KBFX 58 Bakersfield* – (California) **Gas leak forces evacuation of golf course.** A natural gas line sprung a leak June 26 and forced the evacuation of the Sycamore Canyon Golf Course in Arvin, California. A fire spokesman said it was in a main supply line that carries natural gas from the East Coast to the Bay area. Crews from the Kern County Fire Department and Pacific Gas and Electric worked just south of the golf course at the intersection of Tejon Highway and Herring Road to shut down the 34" line. The leak was shut down by PG&E crews around 10:15 a.m. The leak was reportedly caused by a malfunctioning valve.

Source: <http://www.bakersfieldnow.com/news/local/124564429.html>

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

Chemical Industry Sector

4. *June 30, Berkshire Eagle* – (Massachusetts) **1 dead after Williamstown truck crash.** One man died and another was injured on June 28 when a tractor-trailer carrying 44,000 pounds of stearic acid crashed into the woods after it failed to stop at the intersection of Route 2 and Cold Spring Road in Williamstown, Massachusetts, authorities said. The tractor trailer was traveling east on Route 2, around 8:01 a.m. when it failed to stop where the roadway intersects with Cold Spring Road, according to a Williamstown police sergeant. The vehicle was headed to Specialty Minerals in Adams. The fire chief said the impact of the collision caused the tractor-trailer to dump

most of its load. A small amount fell in the brook, while the rest fell onto the driveway of a private home. Stearic acid is a non-hazardous material typically used as a thickening agent in lotions. A crew from the Berkshire County Hazardous Materials Response Team was called to the scene as a precaution, and to provide technical assistance. The company that owns the tractor-trailer also planned to send a crew to help clean up the spill.

Source: http://www.berkshireeagle.com/ci_18381513

For more stories, see items [12](#) and [21](#)

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

Nuclear Reactors, Materials and Waste Sector

5. *June 30, Energy Business Review* – (Pennsylvania) **Unit 2 at Susquehanna nuclear power plant resumes operations.** The Unit 2 at PPL Corporation's Susquehanna nuclear power plant in Luzerne County, Pennsylvania, returned to service June 30 following a refueling and maintenance outage that was extended to replace damaged turbine blades. The planned upgrade work on this unit included installation of an integrated digital control system for plant equipment, and replacement of other turbines that power pumps that provide water to the reactor. The plant's Unit 1 resumed operations the week of June 20 also after a replacement of damaged turbine blades. The Unit 1 reactor was shut down in May after an inspection of the main turbine in the unit revealed blade damage, and similar damage was also found on the plant's Unit 2 turbine.
Source: <http://nuclear.energy-business-review.com/news/unit-2-at-susquehanna-nuclear-power-plant-resumes-operations-300611>
6. *June 30, London Daily Mail* – (International) **Jellyfish swarm forces nuclear power plant to shutdown after they swim into filters.** "High volumes" of jellyfish forced a nuclear power station to shutdown for 2 days after they swam into seawater filters. Staff switched off both reactors at the Torness plant, in Scotland, manually as a precaution. EDF Energy said that they were unsure when the plant in East Lothian would re-open. An EDF spokesman said "'This was a precautionary action and the shutdown cooling systems performed in a satisfactory manner and both reactors were safely shut down."
Source: <http://www.dailymail.co.uk/news/article-2009771/Jellyfish-force-shutdown-nuclear-power-station-swimming-filters.html>
7. *June 30, Professional Reactor Operator Society* – (South Carolina) **Oconee Nuclear Station - NRC inspection report - violation.** A Nuclear Regulatory Commission Violation of Technical Specification 5.4.1.d, for failure to follow procedures was issued June 30 to the Oconee Nuclear Station in South Carolina. The failure to recognize that the condenser off-gas radiation monitors were inoperable was a performance deficiency. This performance deficiency is more than minor because it was associated with the equipment performance attribute of the Mitigating Systems Cornerstone, and adversely affected the cornerstone objective in that the capability to detect, quantify,

and respond to primary to secondary leakage was degraded. The finding did not result in a loss of safety function.

Source: <http://www.nucpros.com/content/oconee-nuclear-station-nrc-inspection-report-violation>

8. *June 29, New York Times* – (International) **Arrests in Moldova over possible uranium smuggling.** Police in Moldova said June 29 they had arrested six people involved with a criminal group that said it was dealing in smuggled nuclear materials, and was active in the former Soviet Union and in Arab countries. The group had been negotiating the sale of uranium, police officials said in a statement, and authorities suggested the material had come from Russia. Some of the suspects were arrested while they were carrying a lead canister. In a video released to news media, police officers wearing gloves showed how a Geiger counter clicked rapidly when brought near the dull gray metal tube. Police said the contents of the tube would be sent for analysis. The Moldovan authorities said that the suspects, who included four Moldovans, one Russian, and one resident of the Russian-backed separatist region of Transnistria in eastern Moldova, had sought a buyer for what the suspects said was bomb-grade uranium.

Source: http://www.nytimes.com/2011/06/30/world/europe/30moldova.html?_r=1

9. *June 29, CNN* – (National) **Mock attackers 'strike' 24 nuclear plants, 'breach' two.** Mock commandos who staged attacks on 24 nuclear power plants in pre-announced drills in 2010 were able to "damage" or "destroy" critical targets at two of the plants, according to the Nuclear Regulatory Commission (NRC.) The NRC did not identify the nuclear plants that failed the security tests, citing security concerns and other sensitivities. But it said inspectors remained at those plants until security shortcomings were addressed. According to an unclassified version of an NRC report released June 29, the NRC conducted force-on-force inspections at 24 nuclear power plants and one nuclear fuel facility during 2010. It identified 23 deficiencies, but none was in the upper range of severity. At two unidentified sites, the utilities failed to "effectively protect" the target during mock attacks, the report said.

Source: <http://www.cnn.com/2011/US/06/29/nuclear.plants.security/>

10. *June 29, WIBW 13 Topeka* – (Kansas) **Wolf Creek nuclear plant expected back online Wednesday night.** The Wolf Creek Nuclear Generating Station near Burlington, Kansas, was scheduled to go back online the night of June 29. The plant has been down since late April for what began as a routine maintenance event. The restart was delayed when the main generator had to be repaired. As of 4:30 p.m. June 29, the plant was at about 7 percent power. A spokeswoman expected it would be synchronized to the power grid, back online, and producing power again by that evening. Wolf Creek had been one of three U.S. nuclear plants under increase oversight from the Nuclear Regulatory Commission. It was taken off that status in late May after passing follow-up inspections.

Source:

http://www.wibw.com/localnews/headlines/Wolf_Creek_Nuclear_Plant_Expected_Back_Online_Wednesday_Night_124749424.html

11. *June 29, Computerworld* – (New Mexico) **Los Alamos shuts down supercomputers as fire advances.** The Los Alamos National Lab shut down two of its largest supercomputers, as wildfires continued to burn near the sprawling New Mexico facility. There were no wildfires on laboratory property June 29, but smoke was prevalent throughout the area. The lab will be closed through June 30. A Los Alamos spokeswoman said the laboratory conducted an "orderly shutdown" of two of its largest supercomputers, IBM's Roadrunner, the first to break the petaflop barrier in 2008, and now the 10th ranked most powerful supercomputer in the world, and Cielo, a Craig system that is ranked No. 6 on the Top500 list. The supercomputer shutdowns were conducted "early on," but an exact day or reason for the action was not clear. The laboratory was first closed June 27 in response to wildfires that have now burned more than 100 square miles. But smoke is a potential threat to data centers and IT equipment. It can trigger a shutdown of air handling systems and IT equipment. Particulates from smoke can damage components. In the case of wildfire activity, the data center would resort to a backup closed loop system. If smoke infiltrated the building, the smoke detectors would shut down the air handling units.

Source:

http://www.computerworld.com/s/article/9218042/Los_Alamos_shuts_down_supercomputers_as_fire_advances

For another story, see item [55](#)

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

Critical Manufacturing Sector

12. *June 30, Wausau Daily Herald* – (Wisconsin) **Northern Wire fined thousands for illegally dumping toxic chemicals in Merrill.** A Merrill company will pay thousands of dollars for illegally dumping toxic pollutants into the Merrill, Wisconsin, sewer system, according to the Wisconsin Department of Justice (WDOJ). Northern Wire was accused of breaking a law that limits the amount of metals that can be released into a sewer system, the WDOJ said. As part of a settlement, Northern will pay \$65,000 in fines and fees. According to a complaint, Northern's wastewater contained large amounts of chromium and zinc that was released into the sewer primarily during the spring and summer of 2009, but also in 2010. The last violation was found February 10. Northern is a custom wire-forming company that uses zinc and chromium in its manufacturing process. Of the 550 samples taken between April 2009 and March 2011, 82 daily violations were found, the complaint said. The violations at Northern Wire were discovered during regular testing of water samples that are sent to the state.

Source:

<http://www.wausaudailyherald.com/article/20110630/WDH0101/106300475/Northern-Wire-fined-thousands-illegally-dumping-toxic-chemicals-Merrill>

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

Defense Industrial Base Sector

13. *June 29, Federal Times* – (Texas) **IG report says Boeing overcharged Army \$13M.** Boeing overcharged the U.S. Army \$13 million on spare parts Army officials could have purchased from the Defense Logistics Agency, according to a Department of Defense Inspector General report released on the Project on Government Oversight's Web site June 28. The Army's Aviation and Missile Life Cycle Management Command bought the 18 parts highlighted in the report, which made up the \$13 million in overcharges. Soldiers and civilians used the parts at Corpus Christi Army Depot in Texas. The depot is a maintenance center used mainly for Army helicopters. After the Defense Department Inspector General released the report, Boeing issued the Army a voluntary refund of \$1.6 million for six types of parts, a Boeing official said. Boeing builds the Army's AH-64 Apache attack helicopter, and the CH-47 Chinook twin-rotor utility helicopter.
Source: <http://www.federaltimes.com/article/20110629/ACQUISITION03/106290303/>
14. *June 29, POLITICO* – (International) **Army's faulty computer system hurts operations.** POLITICO reported June 29 the U.S. Army's \$2.7 billion computing system designed to share real-time intelligence with troops fighting in Afghanistan and Iraq has hurt, rather than helped, efforts to fight insurgents because it does not work properly, according to several analysts who used the system. The analysts' comments mirror concerns raised by the top military intelligence officer in Afghanistan and members of Congress over the past 2 years in an unsuccessful bid to get the Army to consider alternatives to its portion of the military's Distributed Common Ground System (DCGS-A), according to documents obtained by POLITICO. The system is a cloud-based computing network designed to collect information from multiple sources for real-time analysis that quickly puts usable intelligence in the hands of battlefield commanders. The analysts said DCGS-A was unable to perform simple analytical tasks. The system's search tool made finding the reports difficult, and the software used to map the information was not compatible with the search software. There were also problems with the hardware, with the system being prone to crashes and frequently going off-line, he and another former Army intelligence officer said.
Source: <http://www.politico.com/news/stories/0611/58051.html>

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

Banking and Finance Sector

15. *June 30, Kaspersky Lab Security News Service* – (National) **Fake IRS spam campaign pushing Zeus bot.** There is a large scale spam campaign underway in which attackers use fairly well-crafted e-mails that appear to come from the IRS to infect victims with the Zeus bot. The attack has been ongoing for a couple of weeks and researchers said that although the attackers have taken some precautions to prevent analysis of the sites and malware being used, they also made some key mistakes. The Zeus-laden fake IRS e-mails have been making the rounds since mid-June. The subject line typically says, "Federal Tax payment rejected" or "Your IRS payment rejected", and the sender's address is spoofed to include the irs.gov domain. The body of the e-mails often have some spelling and grammatical errors and include a link to a PDF file. That file directs the victim to a download that will drop the Zeus binary on his or her machine.

Source: http://threatpost.com/en_us/blogs/fake-irs-spam-campaign-pushing-zeus-bot-062911?utm_source=Recent+Articles&utm_medium=Left+Sidebar+Blogs&utm_campaign=Dennis+Fisher

16. *June 29, Kalamazoo Gazette* – (Michigan) **Man who claims to be 'Robin Hood Bandit' is to be charged with South Haven Township bank robbery.** A 49-year-old Indianapolis, Indiana man who claimed to be known as the Robin Hood Bandit was scheduled to be arraigned June 29 in U.S. district court after police said he stole \$8,967 from Chemical Bank in South Haven Township, Michigan. He will face one count of armed robbery and one count of brandishing a firearm during a robbery, according to a court filing from the federal court's Western Michigan District in Grand Rapids. On June 25, Bryant allegedly approached a bank teller at about 11:40 a.m. and held up a sign that read, "Let's Go! you only Have 30 seconds!!! All Big Bills!!! 100's \$50's + 20 I will Start Shootin," according to a criminal complaint filed June 27. When South Haven police officers responded to the robbery, they saw the suspect walking out of a wooded area near the bank and carrying a large black bag that was open and full of money. Police also could see a "starting pistol" in the bag. The man was arrested and later confessed to robbing the Chemical Bank, authorities said. "[He] bragged that he had robbed 17 other banks and had been to Federal prison for banks he had robbed in New York and Indiana. He said Federal agents had previously nicknamed him the 'Robin Hood Bandit' because he gave cash to individuals in need," the criminal complaint said.

Source:

http://www.mlive.com/news/kalamazoo/index.ssf/2011/06/man_who_claims_to_be_robin_hoo.html

17. *June 28, Computerworld* – (National) **Federal agency issues new security rules for financial institutions.** The federal agency that regulates banks June 28 issued new rules for online security for financial institutions, instructing them to use minimal types of "layered security" and fraud monitoring to better protect against cybercrime. It is the first time the Federal Financial Institutions Examination Council (FFIEC) has updated its rules since 2005, and the instructions to regulated financial services today focus on protecting high-dollar Automated Clearinghouse (ACH) transactions that have been targeted by sophisticated cybercrime groups that hijack business PCs in order to initiate fraudulent transactions. The FFIEC also instructs banks and financial institutions to focus their network defense on layered security protections that involve fraud monitoring; use of dual customer authorization through different access devices; the use of out-of-band verification; and the use of "positive pay," debit blocks and other technologies to appropriately limit the transactional use of the account. The FFIEC guidelines also tell financial institutions they must use "two elements at a minimum" as "process designed to detect anomalies and effectively respond to suspicious and anomalous activity." The fraud-detection processes must include: initial login and authentication to customers requesting access to the institution's electronic banking system, and initiation of electronic transactions involving the transfer of funds to other parties.

Source:

http://www.computerworld.com/s/article/9217999/Federal_agency_issues_new_security_rules_for_financial_institutions

For another story, see item [32](#)

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

Transportation Sector

18. *June 30, KCTV 5 Kansas City* – (Kansas) **Levee breach closes near Fort Leavenworth airport.** Rising floodwaters breached a Missouri River levee near an airport in Fort Leavenworth, Kansas. A U.S. Army spokeswoman said June 30 the Sherman Army Airfield was closed because of the rising river. Floodwaters undercut the Union Pacific Railroad tracks northwest of the airfield, which is used by civilians and the Army. The military attempted to reinforce the levee, the Army spokeswoman said. In a news release issued June 29, she said the airport is the only area of Fort Leavenworth vulnerable to flooding. She said water reached the hangars, but all salvageable equipment and property were relocated over the past few weeks in anticipation of rising river levels. The breach reached 17 feet wide and 2 feet deep. The estimated cost of damage is unknown, the news release said. Officials were closely monitoring the levels, but did not know yet how high the waters would rise.
Source: <http://www.kctv5.com/story/14998895/flooding-at-sherman-army-airfield>
19. *June 30, Associated Press* – (Nebraska) **Boston-bound jet makes emergency landing in Omaha.** A jetliner carrying nearly 190 people to Boston, Massachusetts, landed safely in Omaha, Nebraska, after a possible engine fuel leak was discovered. Authorities said United Flight 788 landed at Eppley Airfield about 8:20 p.m. June 29. The flight took off from San Francisco, California. Three firetrucks were standing by in Omaha as the jet landed. About 3 hours later, the Boston-bound passengers boarded another United plane and took off. Mechanics were checking the jet engine and the plane's fuel system.
Source: <http://www.beaumontenterprise.com/news/article/Boston-bound-jet-makes-emergency-landing-in-Omaha-1447109.php>
20. *June 30, Los Angeles Times* – (National) **Nigerian stowaway had at least 10 boarding passes, none in his name, officials say.** A Nigerian stowaway who flew from New York to Los Angeles, California with an expired boarding pass in someone else's name was carrying at least 10 different boarding passes, said the FBI agent who took him into custody. Not one of the passes was in the name of the suspect, who acknowledged sneaking aboard a Virgin America flight June 23, officials said. He was arrested as he tried to board a Delta flight from Los Angeles to Atlanta, Georgia, June 29. The crime of being a stowaway is a felony that carries a prison term of up to 5 years, an FBI affidavit said. The FBI became involved June 25, when it "received information from a dispatch operator at the Los Angeles Department of Airports Police and the captain of Virgin America Flight 415," an FBI Special Agent wrote. He said after the flight took off, the suspect was found in a seat that was supposed to be empty. A flight attendant questioned him and he "produced a boarding pass and ticket for the day before and not

in his name," the agent wrote, adding the attendant alerted the captain, who suggested the suspect be asked for additional identification. He hesitated, but then showed identification with his true name, the agent wrote. It was a student ID from the University of Michigan, and the captain noted, the names did not match. The affidavit does not explain why the suspect was not detained on his arrival in Los Angeles. Instead, investigators caught him June 29 when he tried to board Delta Airlines Flight 46 to Atlanta. The suspect had apparently made it through airport security again, having spent the night of June 28 in the airport after passing through security, officials said. He was arrested at the departure gate. The Transportation Security Administration said its review of the matter indicated the stowaway went through physical screening at a security checkpoint. At the Delta gate, the suspect tried to use an expired boarding pass, saying he had missed his flight of the previous day, the same ruse that had worked before, officials said. The suspect said he had been told he could "just go to the gate," according to the affidavit. The Delta agent told him "No," twice, but he kept trying to board. When confronted, the affidavit stated, the suspect "acknowledged that he did not pay for the Virgin America flight." The suspect was in custody in Los Angeles.

Source: <http://latimesblogs.latimes.com/lanow/2011/06/nigerian-stowaway-had-at-least-10-boarding-passes-none-in-his-name.html>

21. *June 30, New York Daily News* – (New York) **Pol blasts inaction on cache of explosive ammo lying in shallow water off Verrazano Bridge.** A diver found an arsenal of unexploded ammunition in underneath the Verrazano Bridge in New York, New York, the New York Daily News reported June 30. The diver discovered the cache in October at the base of the bridge. The 1,500 rounds of ammo, a 3-inch-around projectile and cartridges, are still lying in less than 20 feet of water in Gravesend Bay near the base of the bridge's Brooklyn tower. Starting June 30, new regulations allow the U.S. Coast Guard to block all boats, divers, and fishermen from traveling within 70 yards of the base of the bridge. A temporary safety zone was erected in January.
Source: http://www.nydailynews.com/ny_local/2011/06/30/2011-06-30_pol_blasts_inaction_on_cache_of_ammo_found_under_bridge.html
22. *June 29, New York Times* – (New York) **3 men get 25 years in plot to bomb Bronx synagogues.** Three of the four men convicted in a plot to bomb synagogues in Riverdale in the Bronx borough of New York City were sentenced to 25 years in prison June 29 by a judge in Manhattan, who rejected the government's request for life sentences. In doing so, the judge imposed the minimum sentence. She also reiterated concerns that the government's investigation had raised troubling questions about its tactics and its use of a cooperating witness who posed as a terrorist. But the judge, who had refused to dismiss charges on grounds of government misconduct, said the men were "prepared to do real violence," even though the plot was a government-created sting operation that resulted in no injuries or deaths. The sentencing of a fourth defendant was postponed pending the result of a psychiatric review. All four men were convicted in October 2010 in a case that relied on a government informer who, posing as a Pakistani terrorist, spent months recording discussions with the defendants about placing bombs outside synagogues in the Riverdale neighborhood, and firing Stinger missiles at military transport planes at Stewart International Airport near Newburgh. The charges related to the missiles carried the 25-year mandatory minimum prison

term. Other counts, including conspiracy to use weapons of mass destruction within the United States, carried maximum life sentences.

Source: http://www.nytimes.com/2011/06/30/nyregion/3-men-get-25-years-in-plot-to-bomb-bronx-synagogues.html?_r=2&scp=4&sq=synagogue&st=cse

For more stories, see items [2](#), [4](#), [56](#), [58](#), and [61](#)

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

Postal and Shipping Sector

23. *June 29, Sacramento Bee* – (California) **Sheriff's deputies arrest two in alleged mailbox bombing.** Sacramento County, California sheriff's deputies have arrested two 23-year-old men in connection with the explosion of a device in a residential mailbox June 29. The sheriff's department received a call from a resident who reported hearing a loud explosion. A neighbor also called in and reported seeing somebody place an object in the first caller's mailbox just before the explosion, a sheriff's office release states. The neighbor said the suspect got into a vehicle that fled. Within 10 minutes of the calls, a deputy saw a vehicle matching the suspect vehicle's description and stopped it. Deputies found four occupants and several plastic bottles containing a white powdery substance. Detectives from the sheriff's explosive ordinance detail responded and rendered the devices safe. The suspects were arrested and booked into the Sacramento County Main Jail on suspicion of vandalism, conspiracy, possession of a destructive device, and felony child endangerment, the release said. Deputies reportedly found another device in the mailbox of a residence in the 1800 block of Saint Ann Court in Carmichael. The suspects were each being held in lieu of \$1 million bail, according to online jail booking logs.

Source: <http://blogs.sacbee.com/crime/archives/2011/06/sheriff-two-arr.html>

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

Agriculture and Food Sector

24. *June 30, Reuters* – (International) **Europe's E. coli outbreaks linked to Egyptian seeds.** Imported fenugreek seeds from Egypt may be the source of highly toxic E. coli outbreaks in Germany and France that have killed at least 48 people, according to initial investigations by European scientists. More than 4,000 people across Europe and in North America were infected in the deadliest outbreak of E. coli so far recorded, which started in early May. Almost all of those sickened lived in Germany or had recently traveled there. The German outbreak, and a smaller cluster of E. coli centred around the French city of Bordeaux have both been linked to sprouted seeds. Experts from the Sweden-based European Center for Disease Prevention and Control (ECDC) and the Italy-based European Food Safety Authority (EFSA) said initial investigations suggested that "the consumption of sprouts is the suspected vehicle of infection in both the French cluster and the German outbreak. "The tracing back is progressing and has thus far shown that fenugreek seeds imported from Egypt either in 2009 and/or 2010 are implicated in both outbreaks," they said in a joint statement posted on the ECDC's

Web site late June 29.

Source: <http://www.reuters.com/article/2011/06/30/ecoli-europe-egypt-idUSL6E7HU0EZ20110630>

25. *June 29, WLEX 18 Lexington* – (Kentucky) **Mercer County bar fire ruled arson.** Fire investigators in Kentucky said a fire that destroyed a popular Mercer County bar June 29 was the result of arson. The fire broke out inside Bullfrogs at the corner of Kennedy Bridge Road and Ashley Camp Road. There was nobody inside when the fire started, and there were no reported injuries. The fire cause extensive damage inside the building. Firefighters originally called the fire suspicious. They said a door was open and nobody was around when crews arrived in the scene.

Source: <http://www.lex18.com/news/mercercountybarfire-ruled-arson>

26. *June 29, Foothills Sun-Gazette* – (California) **Beekeeper sting catches honey thief.** The plant manager for a honey farm in Lindsay, California, was arrested June 22 on charges of embezzling hundreds of thousands of dollars worth of raw honey over the course of his nearly 15-year employment. The 55-year-old man from Lindsay was arrested after agents with the Pipkin Detective Agency made a citizen's arrest following a 2-month investigation into the sale of stolen honey from Cary's Honey Farms in Lindsay. The private investigators turned the suspect over to the Tulare County Sheriff's Department's Ag Crimes Unit. An assistant district attorney said the man was charged with one count of grand theft by embezzlement with a special allegation for an amount in excess of \$65,000. He pleaded no contest to all charges at an arraignment June 26. A preliminary hearing was scheduled for July 11. The owner of the honey farm for almost 40 years said he suspected someone was stealing money a few months ago, so he hired Pipkin Detective Agency to uncover the culprit. The investigation provided information that a plant manager was embezzling 55-gallon barrels of honey and selling it to several clandestine packing plants. There it was placed into smaller jars, labeled with fake bar codes, fake phone numbers, and a fake Web site, and then sold to legitimate fruit stands and markets from as far south as Los Angeles to as far north as Merced. Many of the individuals contacted provided additional evidence leading to the arrest of the suspect.

Source: <http://www.thesungazette.com/articles/2011/06/29/news/news01.txt>

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

Water Sector

27. *June 30, Reford Observer* – (Michigan) **Water main breaks disrupt service to many residents.** Redford Township, Michigan, officials continued searching for what caused 16 breaks in water mains the week of June 20, disrupting service to an unknown number of residents. Township officials thought it was highly unusual the week of June 13 when Redford had six water main breaks. Sixteen breaks in a matter of days is "almost unheard of," they said. Eleven of the breaks had been repaired by June 29, the township's director of public services said.

Source: <http://www.hometownlife.com/article/20110630/NEWS16/106300559>

28. *June 29, Jacksonville Journal Courier* – (Illinois) **Boil-water order will extend into July, city now says.** A setback in efforts to return safe drinking water to Jacksonville, Illinois, and outlying communities means it will be July before a boil-water order and conservation constrictions are lifted. City officials said June 29 that the city will not meet the projected date to return to normal water use. Jacksonville and rural water customers who received water from the city were placed under a boil order June 18 after the city's wastewater treatment plant was flooded. The order still includes Scott-Morgan-Greene Water Cooperative, Murrayville-Woodson Water Commission, Alexander Rural Water District, and Manchester.
Source: <http://www.myjournalcourier.com/news/water-33855-city-order.html>

For more stories, see items [1](#), [4](#), [12](#), and [60](#)

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

Public Health and Healthcare Sector

29. *June 30, Associated Press* – (Tennessee) **Thieves get laptop containing patient information in theft from car.** A thief who took a laptop computer from the car of a medical billing company employee got personal information on more than 1,500 patients, the Associated Press reported June 30. An official of PhyData LLC said there is no indication the information had been accessed or misused, according to the Tennessean. The Goodlettsville company bills patients for Advanced Diagnostic Imaging, Premier Radiology and Anesthesia Services Associates. Most of the patients whose information is in the computer received medical services between January 2009 and December 2010. A company spokeswoman said information that includes names, Social Security numbers, medical record numbers of dates of birth is on the laptop, which was stolen from the trunk of an employee's car May 7. PhyData is providing identity theft service to patients whose names are on the laptop.
Source:
<http://www.dailyjournal.net/view/story/a32d7c647e20430e9d12267933d36957/TN--Patient-Information-Stolen/>
30. *June 29, KTVU 2 Oakland* – (California) **Police shoot man who brought gun to senior center.** Suisun City, California police shot and killed a man June 29 who reportedly entered a local senior center with a handgun and later, when confronted by police, aimed it at officers. The man entered the Suisun Senior Citizen Center around 11 a.m. Visitors said an employee spotted him in the lobby, and that he was no stranger. The women said the man was quiet and that they did not know his name. Police said that after the man left the senior center, an employee called 911. Police caught up to the man at the parking lot of the Suisun City Post Office and confronted him. "He was requested to put down the weapon several times by the officers at which time he brandished it ... there was shots exchanged," said the a Suisun City police master sergeant. Police said it did not appear that the man shot at police. Officers fired several times and the man was struck at least once, and died at a hospital.
Source: <http://www.ktvu.com/news/28401678/detail.html>

31. *June 29, Ann Arbor.com* – (Michigan) **Man accused of brandishing stun gun, assaulting U-M hospital worker held on \$100,000 bond.** A man accused of pulling out a stun gun and assaulting a manager at the University of Michigan Hospital cafeteria in Ann Arbor, Michigan, June 24 is being held on a \$100,000 cash or surety bond after being arraigned June 29 at the Washtenaw County Jail. He is charged with unlawful possession of a harmful device, assault with intent to commit great bodily harm less than murder, carrying a weapon with unlawful intent, possession of a stun gun, and assault with a dangerous weapon. University of Michigan police said a masked man approached the manager about 6:40 p.m. June 24 and pulled out a stun gun during an apparent robbery attempt. The man knocked the manager to the ground, leaving him with head and back injuries, a police spokeswoman said. After assaulting the victim, the man ran out the south entrance of the C.S. Mott Children's Hospital, police said. Witnesses told police he left the area on a bus. The victim was treated at the hospital and released that night, the spokeswoman said. The suspect is scheduled to return to court for a preliminary hearing July 6.
Source: <http://www.annarbor.com/news/crime/man-accused-of-pulling-out-taser-and-assaulting-u-m-hospital-worker-is-held-on-100000-bond/>
32. *June 29, WBRC 6 Birmingham* – (Alabama) **Woman charged with stealing information of 4,000 Trinity patients.** A 26-year-old woman from Alabaster has been charged with stealing information from thousands of patients at Trinity Medical Center in Birmingham, Alabama. June 28, a federal grand jury indicted the woman for stealing identifying information from more than 4,000 patients, possessing stolen mail, attempting to commit bank fraud, misusing a Social Security number, and aggravated identity theft, according to a U.S. attorney. She was arrested in early June for a violation of the Health Insurance Portability and Accountability Act (HIPAA) as well as wrongfully obtaining individual health information from Trinity. If convicted of violating the HIPAA statute, she faces a maximum sentence of 10 years in prison and a \$250,000 fine. She faces a maximum prison term of 30 years and a \$1 million fine for attempted bank fraud. For possession of stolen mail and misuse of a Social Security number, she faces a maximum sentence of 5 years in prison and a \$250,000 fine for each charge. If convicted of aggravated identity theft, she must serve 2 years in prison for each count, although those terms might run concurrently with one another.
Source: <http://alabaster.myfoxdal.com/news/crime/woman-charged-stealing-information-4000-trinity-patients/90005>

For another story, see item [39](#)

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

Government Facilities Sector

33. *June 30, KXRM 21 Colorado Springs* – (Colorado) **Haz-Mat incident at Schriever Air Force Base.** A potentially hazardous material incident in Colorado Springs, Colorado left nine Schriever Air Force Base personnel ill June 29. At around 10 a.m., some personnel at the base began complaining of throat irritation. They were evaluated on site and then transported to the hospital for observation. After an examination of the

area by first responders and the Air Force Bio-Environmental Engineers, the building was cleared of any potential hazardous materials. The cause of the incident is under investigation, and all nine people have been released from the hospital.

Source: <http://www.coloradoconnection.com/news/story.aspx?id=635692>

34. *June 29, Seattle Post-Intelligencer* – (Washington) **Men accused of plotting attack on South Seattle federal building to remain jailed.** Two men accused of plotting an attack against a military processing center in Seattle, Washington have been ordered jailed without bail. Charged June 23 with planning a suicidal attack against the East Marginal Way South recruit processing center, a 33-year-old SeaTac-resident and a 32-year-old Los Angeles, California man did not argue for their release during a preliminary hearing June 29. According to the allegations, the 33-year-old was arming himself and two confederates for an attack against the Military Entrance Processing Station, a Department of Defense induction center on East Marginal Way. Authorities learned of the plan after a man asked to join in the attack went to police. Federal prosecutors claim to have the 33-year-old suspect on tape praising terrorists, complaining about American abuses overseas, and preparing to attack the 2-story building. The man and his alleged 32-year-old co-conspirator were charged with planning to storm the center with automatic rifles and grenades. The two men were arrested June 22 and are currently charged with attempting to kill U.S. government officers and employees, and attempting to use a weapon of mass destruction -- a hand grenade -- as well as related offenses. Each faces a minimum sentence of 30 years if convicted as charged.

Source: <http://www.seattlepi.com/local/article/Men-accused-of-plotting-attack-on-South-Seattle-1444558.php>

35. *June 29, KKCO 11 Grand Junction* – (Colorado) **High winds damage community college.** High winds June 28 damaged Northwestern Community College in Rangely, Colorado. The roof of the northwest half of Nichol's Residence Hall was taken off. The roofs of Yeager and Cramer buildings also suffered damage. No one was injured. A tree was also uprooted and fell on the president's residence. The president was in the house at the time, but a spokesperson said he was not hurt. The National Weather Service went to the area to survey the storm area.

Source: <http://www.nbc11news.com/home/headlines/124730739.html>

36. *June 29, WSAZ 3 Huntington/Charleston* – (West Virginia) **Arrest made in copper theft from W.Va. agency.** State Police have arrested a Kanawha County, West Virginia man in connection with a copper theft case that hampered communications June 28 at the West Virginia Department of Agriculture's center in Guthrie. Police said the man ended up knocking out phone and Internet service for the department when he allegedly stole cable near the department's property. Service was restored June 29. Police said they noticed a suspicious vehicle in the area the day of the alleged theft. When police learned of the outage at the agriculture department, they found a red-and-white rope near the site of the damaged lines. Police said they later tracked down the suspicious vehicle and found the same rope tied around the suspect's waist. Police said he did about \$10,000 worth of damage.

Source: <http://www.wsaz.com/news/headlines/124677714.html>

37. *June 29, Bio Prep Watch* – (Indiana; Kentucky) **Army set for large disaster response exercise.** A large disaster response exercise planned by U.S. Army North will take place throughout southern Indiana and northern Kentucky between August 16 and August 28 to train federal military forces for Chemical, Biological, Radiological, and Nuclear (CBRN) incidents. The Vibrant Response 12 and 12A planning conference June 23 in Camp Atterbury, Indiana, was the last chance for those planning the exercise to assemble. The event, which is the fourth field training event in the Vibrant Response series, will help federal forces train in their role in supporting civilian consequent managers in response to chemical, biological, radiological, or nuclear incidents. The 5,200 person Defense CBRN Response Force replaces the 4,500 person CBRN Consequence Management Response Force. It is designed to faster provide more life-saving capability to an incident. Organizations participating in the exercise include the Federal Emergency Management Agency, the Fort Knox Fire Department, the Army's 9th Area Medical Laboratory, National Guard elements from California, Indiana, Michigan, West Virginia, Minnesota, and Illinois, and Verizon Wireless. The DCRF and the similar Command and Control CBRN Response Element A group were created as part of the Department of Defense's transformation of the nation's tiered CBRN response enterprise. The units will assume their mission October 1.
Source: <http://bioprepwatch.com/news/251279-army-set-for-large-disaster-response-exercise>

For more stories, see items [11](#), [22](#), [31](#), and [49](#)

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

Emergency Services Sector

38. *June 30, Peninsula Daily News; Associated Press* – (Washington) **Inmate pair worked together to attempt escape from Clallam Bay, prison officials say.** An inmate serving 45 years for first-degree murder at Clallam Bay Corrections Center in Clallam Bay, Washington was shot to death by a guard as he tried to escape on a forklift while a cohort held a guard hostage June 29. The 25-year-old was shot when he drove a forklift through the doors of the work area and into the perimeter fences, a department of corrections spokesman said. Another correctional officer fired one shot at the man, killing him, he said. State prison officials said June 29 the inmate and a second inmate plotted the escape plan. The other inmate took a correctional officer hostage with a pair of scissors in the laundry and garment area, the spokesman said. While one inmate held the officer, the other took the keys to the forklift from the guard, unchained the machine, and used it to burst out of the building. The inmate followed with the hostage, but surrendered after his fellow inmate was shot, officials said at an evening news conference outside the state prison, which will remain in lockdown into the week of July 4. The correctional officer who was taken hostage was treated for minor injuries, the spokesman said.
Source: <http://www.peninsuladailynews.com/article/20110630/NEWS/306309991/inmate-pair-worked-together-to-attempt-escape-from-clallam-bay>

39. *June 30, Richmond Times-Dispatch* – (Virginia) **Prison lockdown after Va. tuberculosis scare.** A possible tuberculosis case has prompted Virginia officials to lock down the housing unit of a prison in Richmond County. A Virginia Department of Corrections spokesman said June 29 that an inmate was isolated at Haynesville Correctional Center's medical unit June 23 after showing symptoms of the illness. Prison officials contacted the Virginia Department of Health, and face masks were issued to staff and inmates at the locked-down unit. State health officials will conduct mass testing. The spokesman said if no cases were detected, it was hoped the department of corrections will have the unit operating normally before the July 4 weekend for family visitation. Haynesville is a medium- and low-security prison that holds about 1,150 inmates.
Source: http://www.washingtonpost.com/blogs/crime-scene/post/prison-lockdown-after-va-tuberculosis-scare/2011/06/30/AGDKL0rH_blog.html
40. *June 29, WCIV 4 Charleston* – (South Carolina) **Lightning strike takes down 911 call center.** 911 services in Williamsburg, South Carolina were on the fritz June 29 after a lightning strike damaged phone lines, the CAD system, and radio systems within the center. Officials with Williamsburg County said lightning struck the center at about 3:30 p.m. Motorola, Cassidian Communication Inc., and Frontier were hard at work late in the early evening attempting to restore parts of the system. Residents of Williamsburg County were urged to first call 911 in an emergency, but also to call administration lines in the event the 911 call is unsuccessful. Emergency phone lines were re-routed to Clarendon County E-911, where dispatchers were handling calls for Williamsburg County.
Source: <http://www.abcnews4.com/story/15000798/lightning-strike-takes-down-911-call-center>
41. *June 29, CNN* – (Arizona) **Cyberattackers grab more info on Arizona agency employees.** A second hacking attack has yielded personal information belonging to nearly a dozen of its employees, the Arizona Department of Public Safety said June 29. The cyberterrorist group "antisecc" gained access to the personal e-mail accounts of at least 11 employees but did not breach its servers, the department said in a statement. According to a posting on a public Web site, "antisecc" said it had gotten online dating account information, "seductive girlfriend pictures," chat logs, phone numbers, and other personal data and information.
Source:
http://www.cnn.com/2011/CRIME/06/29/arizona.hackers/index.html?hpt=ju_c2
42. *June 29, Associated Press* – (Connecticut) **Federal report faults Bridgeport officials in fire that killed 2 firefighters.** A federal investigation into a house fire last summer that killed two firefighters has determined that city fire officials failed to effectively respond to mayday calls. The report June 29 by the National Institute for Occupational Safety and Health concluded that several factors contributed to the deaths in Bridgeport, Connecticut. It notes that an incident safety officer and rapid intervention team were not readily available on scene, and that ineffective mayday procedures and training also were factors. In February, the state department of labor cited the fire department for serious safety violations, determining that among other problems, it

failed to perform tests on firefighters' breathing gas tanks, failed to conduct medical evaluations, and failed to ensure firefighters were fit. The fire department had a mayday procedure, but it did not test the ability of firefighters, dispatchers, and incident commanders to manage such incidents, the report found. An incident safety officer arrived more than 20 minutes after the initial dispatch because the incident occurred after hours, the report found. Fire departments should ensure a separate incident safety officer is appointed at each structure fire with the initial dispatch, the agency said. Source: <http://www.startribune.com/nation/124741648.html>

43. *June 29, CNN* – (National) **Feuding drug gangs spark violence in Puerto Rico, authorities say.** Power struggles between drug gangs have led to a surge in homicides in Puerto Rico this year, local police and the FBI told CNN. Police statistics show the number of homicides so far this year in the U.S. island commonwealth is 16 percent higher than last year's figure for the same time period — an increase authorities attribute to drug violence. There have been 526 homicides so far in 2011, compared to 452 during the same period in 2010, a Puerto Rico police agent said. Authorities said they suspected drug gangs were behind the slaying of four men who were shot in Rio Piedras June 25. Three of the victims had criminal records related to drug trafficking, police said. Puerto Rico's governor said he plans to implement new technology with "100 percent inspection of trucks entering the island" and centralized systems of DNA to catch criminals. "We have arrested more than 5,960 criminals, dismantled more than 440 points of drugs, and increased our conviction in drug related arrests to 90 percent," his campaign Web site said. This month the department announced it would be creating a new protocol system to "guarantee the civil rights and protections" of all the island's citizens. Source: <http://www.cnn.com/2011/CRIME/06/29/puerto.rico.violence/>

For more stories, see items [37](#), [49](#), and [52](#)

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

Information Technology Sector

44. *June 30, Softpedia* – (International) **WordPress gets new security update.** The WordPress development team released version 3.1.4 of the popular blogging platform to address several vulnerabilities and security issues. The new release fixes a privilege escalation weakness that allows users with Editor levels to gain higher access to the site than usual. WordPress developers credited a member of SEC Consult with discovering and reporting this vulnerability. Two members of the WordPress security team also contributed multiple security fixes and hardening measures for various sorting and ordering functions. In addition to 3.1.4, the development team released the third release candidate (RC3) of the upcoming WordPress 3.2 version. This is expected to be the final release candidate before the new version ships and contains all security patches in 3.1.4 and some additional fixes. The developers write that RC3 includes "few minor RTL, JavaScript, and user interface fixes; and ensures graceful failures if 3.2 is run on PHP4." There is also a reminder that the minimum requirements for the upcoming version will be PHP 5.2.4 and MySQL 5.0.

Source: <http://news.softpedia.com/news/WordPress-Gets-New-Security-Update-208929.shtml>

45. *June 30, Softpedia* – (International) **Vulnerabilities patched in new Joomla release.** The Joomla Project released a new version of its popular CMS platform to address four security vulnerabilities, and two other bugs, Softpedia reported June 30. The new Joomla 1.6.4 version contains patches for two cross-site scripting (XSS) vulnerabilities, one unauthorized access issue, and an information disclosure weakness. The XSS flaws were rated as medium severity and were reported March 24 and May 25. Cross-site scripting is a common vulnerability that results from improper filtering of user input in forms and can result in unauthorized code being injected into pages. There are many types of XSS vulnerabilities with persistent (stored) being the most dangerous because the code injection is permanent. Meanwhile, reflected XSS weaknesses can only be exploited by tricking victims to open maliciously crafted URLs. The Joomla advisories do not specify the type of scripting flaws.
Source: <http://news.softpedia.com/news/Vulnerabilities-Patched-in-New-Joomla-Release-208884.shtml>
46. *June 29, Computerworld* – (International) **Massive botnet 'indestructible,' say researchers.** A new and improved botnet that has infected more than 4 million PCs is "practically indestructible," security researchers said. "TDL-4," the name for both the bot trojan that infects machines and the ensuing collection of compromised computers, is "the most sophisticated threat today," said a Kaspersky Labs researcher in a detailed analysis June 27. The director of malware research at Dell SecureWorks and an internationally-known botnet expert agreed during an interview June 29. The researchers based their judgments on a variety of TDL-4's traits, all which make it an extremely tough character to detect, delete, suppress, or eradicate. The Kapersky Lab researcher said TDL-4 infects the master boot record (MBR) of the PC with a rootkit — malware that hides by subverting the operating system. The master boot record is the first sector — sector 0 — of the hard drive, where code is stored to bootstrap the operating system after the computer's BIOS does its start-up checks. Because TDL-4 installs its rootkit on the MBR, it is invisible to both the operating system, and more importantly, security software designed to sniff out malicious code. What makes the botnet indestructible is the combination of its advanced encryption and the use of a public peer-to-peer (P2P) network for the instructions issued to the malware by command-and-control (C&C) servers.
Source:
http://www.computerworld.com/s/article/9218034/Massive_botnet_indestructible_say_researchers
47. *June 29, Computerworld* – (International) **Google patches 7 bugs in Chrome browser.** Google patched seven vulnerabilities in Chrome June 28 as it issued the second security update for its browser during the month of June. All but one of the flaws fixed in Chrome 12.0.742.112 were rated "high," the second-most-severe threat in Google's four-step ranking system. Several components received patches, including the browser's "V8" JavaScript engine, and the cascade style sheet and HTML parsers. Before June 28, Google last patched Chrome June 8, when it quashed 15 bugs. Three of

the seven vulnerabilities were identified as "use-after-free" bugs, a type of memory management flaw that can be exploited to inject attack code.

Source:

http://www.computerworld.com/s/article/9218020/Google_patches_7_bugs_in_Chrome_browser

48. *June 29, Softpedia* – (International) **Thunderbird 5 contains security fixes.** Mozilla released the next major version of Thunderbird, 5.0, which contains several new features and enhancements, but also many security and stability fixes. Thunderbird 5 was released June 28 and is the first Thunderbird release resulting from Mozilla's new rapid development cycle that aims to produce a new stable version every 6 weeks. The most important change in the new version is it is based on Gecko 5, the same variant of Mozilla's layout engine used by Firefox 5 and, therefore, contains the same security fixes. According to the release announcement, Thunderbird 5 includes "over 390 platform fixes that improve speed, performance, stability and security," however, no other details were released. It can be assumed the new version contains patches for the vulnerabilities addressed in Thunderbird 3.1.11, which was released together with Firefox 3.6.18 the week of June 20.

Source: <http://news.softpedia.com/news/Thunderbird-5-Contains-Security-Fixes-208864.shtml>

For more stories, see items [11](#), [15](#), and [50](#)

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

49. *June 30, IDG News Service* – (International) **LightSquared files GPS report and new plan.** LightSquared filed a long-awaited report on possible Global Positioning System (GPS) interference by its planned cellular network to the Federal Communications Commission (FCC) June 30, along with a formal proposal to use a different block of frequencies to prevent those problems. In a press release announcing the filings, the carrier focused on its new plan and slammed the GPS industry as the cause of the interference. "GPS device test results, which were also filed at the FCC today, show unequivocally that the interference is caused by the GPS manufacturers' decision over the last eight years to design products that depend on using spectrum assigned to other FCC licenses," LightSquared said. The company said its alternative plan, in which it would initially stay out of the portion of its spectrum closest to the GPS band, would solve interference for 99.5 percent of GPS devices in the United States, including all GPS-enabled cell phones. LightSquared has been testing its planned Long Term

Evolution (LTE) network for interference with GPS over the past few months. The Federal Communications Commission required the test report as a condition for letting LightSquared build a hybrid satellite and LTE network across the United States.

Source:

http://www.computerworld.com/s/article/9218056/LightSquared_files_GPS_report_and_new_plan

50. *June 30, Help Net Security* – (International) **Gmail to improve phishing email detection.** Google decided to introduce a change in the way it presents Gmail user with received e-mails. Now, every time a user receives an e-mail from someone who is not in his/her Gmail contacts, the header will automatically show the sender's e-mail address without him having to press the "show details" link. "If the sender's full email address is displayed, then Gmail thinks that you have not communicated with this sender in the past. If the email address is quite long, we'll show you a shortened version," Gmail Help explained. With this change, Google is hoping to help users in detecting phishing and other spam e-mails. "If someone fakes a message from a sender that you trust, like your bank, you can more easily see that the message is not really from where it says it's from," said a software engineer at Google. Also, when Gmail detects a suspicious e-mail or when it seems that someone has spoofed a Gmail address, it will warn the user about it.

Source: <http://www.net-security.org/secworld.php?id=11245>

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

Commercial Facilities Sector

51. *June 30, Madison Capital Times* – (Wisconsin) **Update: Firefighters reenter downtown apartment building looking for hot spots.** Madison, Wisconsin firefighters have reentered the Capitol Hill Apartments building June 30 after eight hours fighting a major blaze downtown, looking for hot spots and any flareups of the fire that has tied up the east side of Capitol Square since dawn. A Madison Fire Department spokeswoman said at 1 p.m. that "the hoses have been turned off for now" in the water attack from outside the walls on the fire that has heavily damaged the 24-unit, three-story apartment building at 24 N. Webster St. The Downtown YWCA residential facility was evacuated after heavy smoke from the fire permeated the building. Residents were allowed back into the building shortly before 2 p.m. The fire spokeswoman said some of the upper level bricks on the Capitol Hill Apartments building have fallen off the structure into an alley, but there was no indication that the walls were going to collapse either into or out from the structure. Motorists are being asked to avoid the east side of Capitol Square. Several streets have been blocked off by Madison police and traffic is being diverted.

Source: http://host.madison.com/ct/news/local/crime_and_courts/article_a14ab7ec-a303-11e0-aafb-001cc4c002e0.html

52. *June 30, Pittsburgh Post-Gazette* – (Pennsylvania) **Massive fire at New Castle factory called suspicious.** A massive fire that ripped through a New Castle, Pennsylvania, factory building June 28 may have been the result of arson, police and fire officials

said. The blaze, which destroyed most of the 34-acre former Shenango China plant near downtown, began around 5:30 p.m. — less than 3 hours after caretakers told police they chased copper thieves off of the property. Fire companies from three neighboring municipalities were called in to assist, and three firefighters were evaluated for possible injuries. The fire was brought under control by nightfall, but the factory, once home to a well-known china company with a long history in New Castle, was seriously damaged. Firefighters and a fire marshal investigated the scene June 29. The city fire chief said the fire hasn't been declared an arson, but he called it suspicious. He said the fire apparently started at multiple locations.

Source: <http://www.post-gazette.com/pg/11181/1157211-54.stm>

53. *June 29, Bangor Daily News* – (Maine) **Fire destroys lobster museum at Bar Harbor Oceanarium.** An iconic museum building visited by thousands of Maine schoolchildren and tourists each year was destroyed June 29 by fire. A Maine Lobster Museum building at the Oceanarium on Route 3 burned to the ground, according to a captain with the Bar Harbor Fire Department. The lobster hatchery and other buildings were not damaged. No one was injured, he said. The initial report of the fire came in about 6:30 p.m., the fire captain said about 9:15 p.m. June 29. He did not know who reported the fire. Firefighters from Trenton, Mount Desert, and Southwest Harbor assisted in fighting the blaze. The fire captain said a crew would remain at the Oceanarium until late June 30 or early July 1.

Source: <http://bangordailynews.com/2011/06/29/news/hancock/firefighters-battle-oceanarium-blaze-in-bar-harbor/>

54. *June 29, Indianapolis Star* – (Indiana) **Propane leak forces evacuations on Southside.** Indianapolis firefighters evacuated businesses in an Indianapolis, Indiana industrial area June 29 where a propane tank ruptured and was leaking. The leak was at the OmniSource facility, a scrap metal recycling plant, at 2155 S. West Street, and the evacuation was about a half mile in all directions, said an Indianapolis Fire Department spokeswoman. About 75 OmniSource employees were evacuated without injury, she said. The leak happened at 2 p.m. when a large piece of metal being hoisted by a crane fell to the ground and sent shrapnel into a high-pressure propane tank, she said. It caused a 2-inch diameter gash in the rounded end of the tank, she said. The tank was venting, and by 5 p.m. it was down to about 25 percent of volume, the spokeswoman said. A 3,000-gallon liquid oxygen tank is next to the propane tank, heightening the concern about safety, she said. Fire department personnel have been moved to a safe zone outside the plant, the spokeswoman said. Crews also were monitoring air quality in the area, but fire officials said the vapors appeared to be dissipating.

Source: <http://www.indystar.com/article/20110629/LOCAL18/106290357/Propane-leak-forces-evacuations-Southside?odyssey=mod|newswell|text|Communities|s>

For more stories, see items [3](#), [22](#), [37](#), [55](#), [60](#), and [61](#)

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

National Monuments and Icons Sector

55. *June 30, CNN* – (New Mexico) **Officials hopeful as Los Alamos fires rage; lab closed.** Firefighters in New Mexico have not yet gotten the upper hand against the Los Alamos fire, officially called the Las Canchas fire, which is burning near the Los Alamos nuclear lab. But a sense of accomplishment was evident as the battle headed into June 30. "We're in the best shape since this thing started," said the fire chief, who told reporters June 29 was make-it-or-break-it day. Even with the progress, the nearby flames will keep the Los Alamos National Laboratory closed through at least July 1, a statement on the lab's Web site said. The fire has forced nearly 10,000 people from their homes in the town. Officials estimate the fire has consumed about 70,000 acres. The operations section chief for the multi-state southwest area incident management team, said fire officials plan to flank the fire on the east side June 30 in an attempt to curb high winds predicted from the southwest. The Las Conchas fire was one of several burning in the region. The Donaldson and Game fires south of the town of Hondo and U.S. Highway 70 have merged into one fire that has consumed about 43,290 acres and is zero percent contained, according to the New Mexico Fire Information Web site. Evacuations were ordered June 29 for Alamo Canyon as the Donaldson fire continued to threaten parts of Lincoln County. The Pacheco fire continued to burn in the Pecos Wilderness, 2 miles north of the Santa Fe Ski Basin. It has scorched 10,000 acres since it began June 18. The blaze was 24 percent contained early June 30, with the potential for growth considered low, according to InciWeb.

Source:

http://www.cnn.com/2011/US/06/30/new.mexico.los.alamos/index.html?hpt=hp_t2

56. *June 30, WBRC 6 Birmingham* – (Alabama) **Florida firefighters aid efforts against Gulf State Park blaze.** Some Florida fire crews were helping Alabama firefighters extinguish the brush fire that is burning in Gulf State Park in Alabama. The fire is directly affecting about 250-acres, but is also forcing some road closings, which are causing other problems for tourists and locals.

Source: <http://www.myfoxdal.com/story/15003188/florida-firefighters-aid-efforts-against-gulf-state-park-blaze>

57. *June 29, KUSA 9 Denver* – (Colorado) **2 fires break out in windy Boulder area.** Two fires started burning in the Boulder, Colorado area the afternoon of June 29, and people in several homes were warned they may have to evacuate because of one of the fires. Authorities said the Coffintop Fire was along Highway 7 near mile marker 31. It was about 30 to 40 acres in size and 5 percent contained, June 29. Air support was being used to help fight the fire. The U.S. Forest Service (USFS), a Type 3 incident management team, and Boulder County firefighters were on scene. They planned to stay on the fire line overnight. About 15 homes received emergency notification messages that they may have to evacuate. Half of the fire is on USFS land, and the other half is on Boulder County land. The other fire is the Blue Mountain Fire, which is in Larimer County northwest of Lyons. It is off of Blue Mountain Road, near Highway 36. It is about 5 acres in size. Authorities believe the fire was starting to die down. Fire crews were concerned by the high wind gusts in the area. The USFS began Stage 2 fire restrictions June 29 in the Pike & San Isabel National Forests, Cimarron & Comanche National Grasslands because of the severe wildfire threat in southern Colorado.

Source: <http://www.9news.com/news/article/205748/339/2-fires-break-out-in-windy-Boulder-area>

58. *June 29, Jacksonville Daily News* – (North Carolina) **Burn out helps increase containment to 68 percent.** The fire in the Holly Shelter Game Lands in North Carolina is 68 percent contained, forestry officials said June 29. Forestry had burned off almost 15 miles of the fire's 40-mile perimeter by June 28, an information officer with the North Carolina Forest Service (NCFS) said. Forestry completed most of the large-scale burnouts it planned to do, he said. Due to the 8,000-acre burnout, containment went from 30 percent to 68 percent June 29, when 208 personnel worked the fire. The fire has consumed 30,593 acres. Crews continued with mop up operations June 29, checking the lines from the burnout, and working on contingency lines north of the fire. Two dozer strike teams, consisting of four dozers and personnel from Camp Lejeune, were released. There is a potential for a super fog, a combination of super dense smoke and fog, June 30 in the early morning hours, a NCFS information officer said, though it will mainly effect I-40 and the Wilmington area. Motorists should remain cautious and allow for extra travel time. Forestry was working with emergency services, highway patrol, and local sheriff's departments to monitor the smoke on area roadways in the event road closures are necessary.

Source: <http://www.jdnews.com/news/-92671--.html>

For another story, see item [11](#)

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

Dams Sector

59. *June 30, KXTV 10 Sacramento* – (California) **Sierra dam cracks worries residents.** A close look at the Lake Van Norden Dam in Soda Springs, California shows a large, leaking crack across part of its face and a torrent of water pouring from below the northern edge of the dam. Residents downstream are worried about potential failure. The Nevada County Emergency Services director said the county is not certain who owns the dam, but staffers plan to find out and see if the dam has been getting regular safety inspections. Part of the dam was breached many years ago to allow a freer flow of water, but the dam still holds back a sizeable amount of water in what remains of Lake Van Norden.
- Source: <http://www.news10.net/news/local/article/143947/2/Sierra-dam-cracks-worries-residents>
60. *June 30, Winnipeg Free Press* – (North Dakota; International) **Dike-building becomes 24/7 work in Souris.** As the Souris River begins to rise in Melita, North Dakota, flood-fighting efforts moved downstream to Plum Creek, where the surge rose significantly, backing up where it enters the Souris. A dike was built to protect a greenhouse, nine homes, and the water-treatment plant before the predicted crest of the river between July 7 and 10 at an estimated 1,368 feet. The 24/7 dike work is expected to last for several days to catch up to the crest deadline. The National Weather Service increased the forecast peak flow in Westhope, North Dakota, to 30,142 cubic feet per second (cfs)

July 4, which is an increase of about 300 cfs over its June 27 forecast. A flood warning for all reaches of Pipestone Creek and downstream into the Oak and Plum lakes system, then on Plum Creek to the Souris River, including the town of Souris was issued. The Assiniboine River upstream of the Souris in the Canadian provinces of Saskatchewan and Manitoba, is expected to experience another peak at the beginning of July. The flow upstream of Portage la Prairie is forecast to remain at or near the current flow of 38,000 cfs for a few days before it starts to rise in response to the large flows from the Souris River basin. The Qu'Appelle River in Saskatchewan crested June 29 at 9,700 cfs, which is an earlier and lesser crest than the Saskatchewan Watershed Authority's recent forecast that a crest of 11,500 cfs would occur.

Source: <http://www.winnipegfreepress.com/local/dike-building-becomes-247-work-in-souris-124763214.html>

61. *June 30, Omaha World-Herald; Associated Press* – (Iowa; Nebraska; Missouri)
Another levee breach in S.W. Iowa. A 200-foot breach of a Missouri River levee 2.5 miles northwest of Percival, Iowa, started around 3 or 4 a.m., June 30, said the Fremont County Emergency Management director. The National Weather Service said the breach was discovered after the river level downstream at Nebraska City, Nebraska, dropped about 6 inches, to 27.6 feet. On-site reports showed about 5 feet of water across 200th Street. Local officials said the water flowing through the breached levee could eventually join the flood waters from failed levees south of Hamburg, which could increase the pressure on Hamburg's new levee. The waters could affect 24 homes south of the breach, officials said. I-29 is now closed from exit 24 near Bartlett, Iowa, south to Rock Port, Missouri.

Source: <http://www.omaha.com/article/20110630/NEWS01/110639992/538>

For another story, see item [18](#)

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

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 cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267

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.