

UNCLASSIFIED



NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Regional](#)

[National](#)

[International](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[Commercial Facilities](#)

[Communications Sector](#)

[Critical Manufacturing](#)

[Defense Industrial Base Sector](#)

[Emergency Services](#)

[Energy](#)

[Food and Agriculture](#)

[Government Sector \(including
Schools and Universities\)](#)

[Information Technology and
Telecommunications](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Public Health](#)

[Transportation](#)

[Water and Dams](#)

[North Dakota Homeland Security
Contacts](#)

UNCLASSIFIED

NORTH DAKOTA

Water intake system work under way. Work on Bismarck, North Dakota's new \$16 million water intake system resumed this summer after it was delayed a year due to the 2011 Missouri River flood. The water collection system will bring purer water back to the city's water treatment plant and increase its intake capacity, said the director of utility operations for the city. —Structural steel is being placed on top of the well that was built in 2010. It's the support of the pumping station, he said. The pumping station enclosure should be completed sometime between November and the end of 2012. The new system will allow water collection capacity to increase from 30 million gallons allowed now to 35 million gallons, according to officials. The existing water intake system will act as a backup in emergencies and when demand exceeds the new intake system's storage capacity. Source: http://bismarcktribune.com/news/local/water-intake-system-work-under-way/article_40935af2-f380-11e1-86fa-0019bb2963f4.html

Williston sewage problem. KFVR 5 Bismarck reported August 27 that the Williston, North Dakota sewage plant was experiencing capacity issues. —The plant is running probably 25 percent over the design capacity, said the Williston public work director. —What would happen is if you're running over that you just don't have enough storage time in those ponds to hold it long enough to meet your discharge parameters. Recently, upgrades at the plant put in brand new pumps that can process thousands of gallons of water per minute. Step two of expansion is under construction. The treatment plant gets about 2 million gallons of water every day, and it is treated in ponds with oxygen, and then shipped to lagoons. But when the temporary plant opens it can be shipped to the lagoons or the temporary plant. And the temporary plant will feed the water to the backwaters of the Missouri river. The third step is to build a permanent waste water plant that will be able to meet the city's needs. The permanent plant is still a few years away. Source: http://www.kfyrtv.com/News_Stories.asp?news=58944

Souris River levee system to get final repairs. The U.S. Army Corps of Engineers awarded a contract to complete repairs to Souris River levees in Minot and Burlington, North Dakota, damaged by historic flooding during the summer of 2011, the Associated Press reported August 23. Construction is to be completed by the end of 2012. The Corps has spent nearly \$3 million fixing the levee system since the 2011 flood. The agency said that once the final repairs are done, residents will have the same flood protection they had before the flood. Separately, a U.S. Senator said the Corps is giving Minot \$1.9 million for sanitary sewer repairs. Source: <http://www.grandforksherald.com/event/article/id/243491/group/homepage/>

Area water safe after sewage dump in Sheyenne. The North Dakota Health Department said residents of Fargo should not worry about their tap water despite sewage being dumped into the Sheyenne River August 16 and 17 in Valley City. The metro area takes in water from the river, but at the time of the event, Fargo water officials said they were not doing so. Valley City was rerouting sewage water from a malfunctioning lift station into the Sheyenne for about 30 hours starting the morning of August 16, but the issue was corrected by the afternoon of August 17. During routine maintenance on the city's main sewage well, the plug on the master

UNCLASSIFIED

drain failed and flooded the station. Six pumps used to move sewage from the well into the city's sewage lagoon were inundated causing major backups. Two of the pumps were fixed. If not for the "heroic" work of the staff on hand, an official said, hundreds of homes could have seen serious damage. To prevent this, they began pumping the contents of the flooded station into the Sheyenne, he said. Officials said increased water flows from Devils Lake helped to dilute the river water and decrease the impact of the sewage. Source:

<http://www.jamestownsun.com/event/article/id/167377/group/News/>

REGIONAL

(Minnesota) Salmonella linked to turkey jerky sickens 4 in Minnesota. Four cases of Salmonella infection were linked to turkey jerky produced by a Minnesota company, Food Safety News reported August 23. The Minnesota Department of Health (MDH) warned consumers not to eat whole-muscle turkey jerky manufactured by Hoffman Town & Country Meat Market because investigators linked the product to a cluster of four illnesses from the same strain of Salmonella. The first patient became ill August 2 and the last illness onset was August 7, stated the MDH. One of the victims was hospitalized but all have since recovered. All four victims reported eating turkey jerky during the week before becoming ill. Hoffman Town & Country issued a voluntary recall of all whole muscle turkey jerky sold on or before August 21. The product was sold wrapped in white butcher paper. Source:

<http://www.foodsafetynews.com/2012/08/four-cases-of-salmonella-infection/#.UDeHzaC6TIY>

(Wyoming) Wyoming faces worst hay crop in decades. Wyoming is facing one of its worst hay harvests in terms of acreage in nearly 80 years, according to new U.S. Agriculture Department (USDA) estimates, the Associated Press reported August 18. Hay is Wyoming's biggest cash crop, and it also is suffering the most from a lack of rain earlier in the season. USDA crop yield estimates released late the week of August 13 project Wyoming's overall hay harvest in 2012 to yield about 925,000 acres of hay. If realized, that would make 2012 the single worst year for Wyoming hay acreage since the Dust Bowl days of 1934. The overall tonnage of hay expected to be harvested in Wyoming is 1.82 million tons, down 23 percent from 2011 and the worst production since 2002. Other crops are faring better, particularly sugar beets and dry edible beans. Yields are expected to rise by 23 and 36 percent, respectively. The poor hay crop has sent hay prices soaring, according to the director of the USDA National Agricultural Statistics Service office in Cheyenne. He said that 79 percent of the pasture and grazing lands in Wyoming are rated "poor" to "very poor." Source: http://trib.com/news/state-and-regional/wyoming-faces-worst-hay-crop-in-decades/article_b9a19955-6807-5190-9656-48f381fa97ae.html?comment_form=true

NATIONAL

Second accused LulzSec hacker arrested in Sony Pictures breach. A second suspected member of the clandestine hacking group LulzSec was arrested August 28 on charges he took part in an extensive computer breach of Sony Pictures Entertainment, the FBI said. The suspect of Tempe, Arizona, surrendered to U.S. authorities in Phoenix 6 days after a federal grand jury in Los

UNCLASSIFIED

UNCLASSIFIED

Angeles returned an indictment charging him with conspiracy and unauthorized impairment of a protected computer. If convicted, the suspect faces up to 15 years in prison. The indictment accused the suspect and co-conspirators of stealing data from Sony Corp's Sony Pictures' computer systems in May and June 2011 using an —SQL injection attack against the studio's Web site, a technique commonly employed by hackers. The indictment said the suspect then helped post the confidential data onto LulzSec's Web site and announced the intrusion via the hacking group's Twitter account. The FBI said his co-conspirators included a confessed LulzSec member who pleaded guilty in April to federal charges stemming from his role in the attack. Following the breach, LulzSec published the names, birth dates, addresses, emails, phone numbers, and passwords of thousands of people who had entered contests promoted by Sony, and publicly boasted of its exploits. Authorities have said the Sony breach ultimately cost the company more than \$600,000. Source: <http://www.reuters.com/article/2012/08/29/us-usa-hacking-lulzsec-idUSBRE87S03520120829>

INTERNATIONAL

Floods displace 20,000 in Nigeria after dam opened. Flooding in eastern Nigeria killed at least 10 people and displaced an estimated 20,000 following heavy rains and the release of water from a dam in neighboring Cameroon, an official said August 27. He said water was released from the Lagdo dam August 24 in Cameroon after officials there warned Nigeria several weeks ago. The opening of the dam led to flooding along the Benue River in Nigeria. —The people along the Benue River were advised to leave but did not heed the warning, he said. —Thousands of hectares of crops and homes were destroyed in the flooding. We have started a situation assessment to see how best we can assist the affected people. Flooding this rainy season in various parts of Nigeria, Africa's most populous nation with 160 million people, had already killed dozens. Much of the country has been affected by heavy seasonal rainfall. The flooding also raises the risk of the spread of diseases such as cholera. Source: <http://www.deccanchronicle.com/channels/world/africa/floods-displace-20000-nigeria-after-dam-opened-717>

Mexico's big oil problem. Mexico, one of the largest suppliers of oil to the United States, is gradually declining in its production of crude oil. In 2008, the country's production peaked at 3.2 million barrels a day, according to the U.S. Energy Information Administration (EIA). In 2011, it produced under 3 million a day. The reason is due to aging oil fields and years of underinvestment. Industry experts say Mexico could revive production if it allowed more investment from international oil companies. But under current policy, EIA says Mexico will have to start importing oil by 2020. For the United States, the decline in Mexico's oil industry means it will likely be buying more oil from Canada and Saudi Arabia, the number 1 and 2 sources of U.S. oil imports. The loss of Mexico's current exports of about 1 million barrels a day would be greater than the amount lost due to sanctions on Iran, albeit over a longer time period. Many experts blame the structure of Mexico's oil industry for the decline. Source: http://money.cnn.com/2012/08/17/news/economy/mexico-oil/index.html?source=yahoo_quote

UNCLASSIFIED

BANKING AND FINANCE INDUSTRY

Curbing card fraud at the pump. Card fraud linked to pay-at-the-pump gas terminals is growing, and that trend will continue until more fraudster convictions are publicized, some security experts say, according to BankInfoSecurity August 31. Meanwhile, in an effort to help prevent fraud, one trade association is testing a system designed to help alert convenience stores and others about potential skimming threats. A fraud expert at Aite said that many card issuers speculate that the increases are linked to crime rings that want to exploit the card data they have in-hand before the U.S. payments infrastructure migrates to chip-card technology, part of a movement to comply with the global Europay, MasterCard, Visa standard. To help combat skimming, the Petroleum Convenience Alliance for Technology Standards (PCATS) is beta-testing a skimming database that logs reports of pay-at-the-pump skimming incidents. PCATS is working with about 10 retail and petroleum brands to collect data that can be used to identify common targets. Once regions or certain terminal brands have been identified as being hit by skimming most often, PCATS notifies other convenience stores and gas stations that are likely to be the next victims. Source: <http://www.bankinfosecurity.com/curbing-card-fraud-at-pump-a-5080/op-1>

1 Million accounts leaked in megahack on banks, websites. Hacker collective Team GhostShell leaked a cache of more than 1 million user account records from 100 Web sites over the weekend of August 25, The Register reported. The group, which is affiliated with the hacktivist group Anonymous, claimed they broke into databases maintained by banks, U.S. government agencies, and consultancy firms to leak passwords and documents. Some of the pinched data included credit histories from banks among other files, many of which were lifted from content management systems. Some of the breached databases each contained more than 30,000 records. An analysis of the hacks by security firm Imperva revealed that most of the breaches were pulled off using SQL injection attacks. Source: http://www.theregister.co.uk/2012/08/28/team_ghostshell_megahack/

Cybercrooks fool financial advisers to steal from clients. Cybercriminals are using falsified email messages in attempts to con financial advisers into wiring cash out of their clients' online investment accounts, USA Today reported August 26. If the adviser falls for it, a wire transfer gets legitimately executed, and cash flows into a bank account controlled by the thieves — leaving the victim in a dispute with the financial adviser over getting made whole. Anecdotal evidence of this ruse — directed at financial planners, estate lawyers, and other advisers who rely on email and online banking to work with clients — has just begun to surface, according to tech security and online banking experts. IDentity Theft 911, a theft-recovery service, is working on a case where a faked email led to a \$35,000 transfer. In another caper, a veteran financial planner was fooled by a Gmail message appearing to arrive from an insurance company executive. The email carried instructions to wire \$15,850 into an account at PNC Bank, worded in a casual style similar to past emails the adviser had received from the executive. Luckily, the planner phoned his client to clarify which account to pull the money from and discovered the fraud. Cybercriminals have discovered investors now routinely rely on email to authorize personal advisers to execute financial transactions. —Instead of managing layers of malicious

UNCLASSIFIED

software, all the bad guys need is e-mail and phone skills , a vice president at Authentify said. Source: <http://www.usatoday.com/tech/news/story/2012-08-26/wire-transfer-fraud/57335540/1>

FTC wins \$478 million award in ‘easy money’ scam case. The U.S. Federal Trade Commission (FTC) said the operators of three “get-rich-quick” systems were ordered to pay \$478 million for deceiving almost 1 million consumers with phony money-making claims, Bloomberg News reported August 23. The court order represents the largest litigated judgment ever obtained by the agency and is part of its effort to stop scams that prey on financially distressed consumers, the FTC said. One system was sold with the promise that customers could “quickly and easily earn substantial amounts of money by purchasing homes at tax sales in their area „free and clear“ for just „pennies on the dollar,“ and then turning around and selling these homes for full market value or renting them out for a profit,” the FTC said in its June 2009 complaint. John Beck Amazing Profits LLC, John Alexander LLC, and Jeff Paul LLC were among the defendants. The court found that despite the marketers’ claims, almost all of the consumers who bought the \$39.95 systems lost money. Source: <http://www.businessweek.com/news/2012-08-23/ftc-wins-478-million-award-in-easy-money-scam-case>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Tennessee) Troubling ineptitude in security at US nuclear bomb plant. Guards at the Oak Ridge, Tennessee plant for storing weapons-grade uranium failed to spot activists who cut through its fences until they walked up to an officer’s car and surrendered, an official report said August 31. The report from the Department of Energy’s (DOE) inspector general criticized multiple failures of sophisticated security systems and —troubling displays of ineptitude at the plant in July. Three anti-nuclear activists were not initially spotted or detained as they cut through three perimeter fences July 28. The officer responding to the alarm did not notice the trespassers until they walked up to his car and —surrendered. The officer did not draw his weapon nor secure the area, instead letting the trespassers —roam about and retrieve various items from backpacks, the report said. Another officer hearing alarms did not look outside the building as he was supposed to, and also missed an image of the trespassers on a camera. A third officer turned off the alarm. Others heard the activists hammering on the building’s outside wall, but assumed the sound was from maintenance workers. One camera that would have shown the break-in had been broken for about 6 months, and there was a backlog of repairs needed for security systems at the facility, the report said. The administrator of the National Nuclear Security Administration said changes were underway after the incident. He said that staff members involved with the incident were removed, cameras were fixed, and patrols as well as training were stepped up. Source: <http://www.reuters.com/article/2012/08/31/usa-security-nuclear-idUSL2E8JV7PD20120831>

(California) Ailing Calif. reactor prepares to remove fuel. The operator of the San Onofre nuclear power plant in San Diego County, California, is preparing to empty the fuel from one of its twin reactors, a Nuclear Regulatory Commission inspector said August 27, which is another sign the plant would not be operating at full capacity anytime soon. Tons of fuel inside the

UNCLASSIFIED

UNCLASSIFIED

disabled Unit 3 reactor will be moved into storage in mid-September. The plant has been shut down since January after a break in a tube that carries radioactive water. Investigators later found unusual wear on scores of tubes inside the plant's four steam generators, and Southern California Edison has been trying for months to determine how to fix it. Edison has previously said it is focusing on repairing the Unit 2 reactor, which had been taken offline earlier in January for maintenance, and that —the Unit 3 reactor will not be operating for some time. Source: http://seattletimes.com/html/nationworld/2019004570_apusnuclearplantproblems.html

COMMERCIAL FACILITIES

(New York) Security upgrades under way at municipal buildings. Niagara County, New York, was continuing its efforts to improve security at county-owned buildings through construction of additional barriers. Work began the week of August 20 on a new security door in the hallway next to the county legislature chambers in the county courthouse to block access to the legislature chairman's and clerk's offices. The county risk management director said a similar door will be installed in the hallway on the other side of the legislature chambers leading to caucus rooms and the county mailroom. She said the projects, done by county public works employees, are part of a series of security-related improvements on county properties since the State Workplace Violence Protection Act went into effect in September 2009. —There was some hardening we needed to do, she said. —They were concerned about shootings and issues at workplaces. It was mostly because of domestic violence incidents spilling over into Social Services offices. Source: <http://www.buffalonews.com/city/communities/niagara-county/article1024652.ece>

(Illinois) Two guests of JW Marriott in Chicago die from Legionnaires' disease. Two guests of the JW Marriott in downtown Chicago died from Legionnaires' disease, WBBM 2 Chicago reported August 28. There have been five new cases of the disease on top of three reported cases the week of August 20. —We believe that there is no ongoing health threat at the hotel, a representative from the Chicago Department of Public Health said in a press release. It urged people who stayed at the hotel experiencing flu-like symptoms to contact a healthcare provider. The week of August 20, WBBM reported that three out-of-state guests at the hotel developed the disease caused by water-borne Legionella bacteria. One of the dead included a Florida physician initially thought to have died from pneumonia until his family received a letter from the hotel notifying of the outbreak, which led to an autopsy that confirmed Legionnaires'. Victims were thought to be exposed to the bacteria between July 16 and August 15. About 8,500 people were guests of the hotel during this time. Source: http://www.cbsnews.com/8301-504763_162-57501589-10391704/two-guests-of-jw-marriott-in-chicago-die-from-legionnaires-disease/

(New York) Empire State Building shootings kill 2 and wound 8, police say. A disgruntled former worker sparked chaos in front of the Empire State Building in New York City August 24 when he shot and killed a co-worker and engaged in a gun battle with police that left at least eight others wounded, authorities said. The shooter was killed in an exchange of gunfire with two police officers just as visitors began to queue up to ascend the famous skyscraper. The

UNCLASSIFIED

UNCLASSIFIED

officers fired 14 rounds after the suspect apparently turned his gun on them, said the New York police commissioner. Some of the wounded people may have been hit in the crossfire or by ricocheting bullets, he said. The suspect was apparently laid off from his job as a designer of women's accessories at Hazan Imports in 2011. Dressed in a business suit and carrying a briefcase, he apparently had a longstanding dispute with the victim over allegations of harassment in the workplace, police said. Both men had filed prior complaints. A construction worker followed the gunman after the initial gunshots and alerted officers. Two police officers were being treated at a hospital, though no injuries are considered life-threatening, the New York mayor said. The suspect used a .45-caliber semiautomatic handgun and was carrying extra ammunition in his briefcase, stated police. Local and federal authorities who converged on the building around 9 a.m. closed several streets around 5th Avenue and 34th Street, snarling traffic in the heart of Manhattan. Shortly after the incident, a medical center reported it was treating six victims suffering from gunshot wounds. All the injuries were not life threatening, stated a hospital spokeswoman. Source: <http://www.cnn.com/2012/08/24/justice/new-york-empire-state/index.html>

COMMUNICATIONS SECTOR

Nothing Significant to Report

CRITICAL MANUFACTURING

BatteriesPlus expands recall of battery packs used in cordless tools due to explosion hazard.

The U.S. Consumer Product Safety Commission, in cooperation with BatteriesPlus LLC, August 30 announced a voluntary recall of about 65,300 Rayovac NI-CD and Rayovac NI-MH Cordless Tool Battery Packs. Consumers should stop using recalled products immediately. About 111,800 battery packs were also recalled in December 2011. The replacement battery pack can explode unexpectedly, posing a risk of injury to consumers. BatteriesPlus has received three additional reports since the previous recall of exploding batteries, including one report of an injury to a consumer's finger. The battery packs were sold exclusively at BatteriesPlus retail stores and online at the BatteriesPlus Web site between June 2008 and July 2012. Consumers can contact BatteriesPlus for instructions on how to return the product for store credit. Source:

<http://www.cpsc.gov/cpsc/pub/prerel/prhtml12/12267.html>

Mr. Coffee single cup brewers recalled by JCS due to burn hazard. The U.S. Consumer Product Safety Commission and Health Canada, in cooperation with Jarden Consumer Solutions (JCS), August 30 announced a voluntary recall of 600,700 Mr. Coffee Single Cup Brewing Systems sold in the United States and Canada. Consumers should stop using recalled products immediately. A build-up of steam in the water reservoir can force the brewing chamber open and expel hot coffee grounds and water, posing a burn hazard. JCS has received 164 reports of the brewing chamber opening due to steam pressure, including about 59 reports in the United States and 2 in Canada of burn injuries to consumers' face, upper torso and hands. Consumers should stop using the recalled coffee brewer and contact JCS to receive instructions on how to obtain a free replacement unit. Source: <http://www.cpsc.gov/cpsc/pub/prerel/prhtml12/12263.html>

UNCLASSIFIED

UNCLASSIFIED

Judge stops ex-Toyota worker from leaving country. A federal judge in Lexington, Kentucky, ordered a former computer programmer for Toyota from leaving the United States while the company investigated damage done by an alleged computer hacking incident, the Associated Press reported August 27. The judge also ordered the man to forfeit any data he took from the computer system of Toyota Motor Engineering & Manufacturing North America. In a lawsuit filed in federal court, Toyota alleged the man illegally accessed the Web site toyotasupplier.com after being dismissed from his contract position August 23. The company claims he reset the Web site and computer system to automatically crash. At that point, Toyota alleged, the man, a native of India, accessed Toyota's internal computer system without authorization and copied, downloaded, and possibly disseminated trade secrets and proprietary data. Included in that information was pricing information, quality testing data, and parts testing data, Toyota's attorney wrote in the complaint. Toyota also claimed he reprogrammed at least 13 applications the computer system to cause it to crash, and also removed critical security certifications on the company's internal server, causing the programs to become inoperable. He was unsure how long it would take for Toyota's technology department to repair the damage. Source: <http://www.sfgate.com/business/article/Judge-stops-ex-Toyota-worker-from-leaving-country-3818233.php>

NHTSA recall notice - Chevrolet Sonic windshield wiper washer hoses. General Motors (GM) announced August 27 the recall of 44,668 model year 2012 Chevrolet Sonic vehicles manufactured from May 5, 2011 through February 24, 2012. The windshield wiper washer hose on these vehicles may separate from the washer fluid reservoir. If this occurs, washer fluid will not be available to the windshield. A lack of washer fluid could impede the driver's view, increasing the risk of a crash. GM will notify owners, and dealers will secure the windshield washer hose to prevent separation. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V408000&summary=true&prod_id=1361768&PrintVersion=YES

Insight: Experts hope to shield cars from computer viruses. Several companies and organizations are working to protect the computer systems of cars from compromise and attack, Reuters reported August 20. Intel's McAfee unit is one of a handful of firms that are looking to protect the dozens of tiny computers and electronic communications systems that are built into every modern car. Security experts said automakers have so far failed to adequately protect these systems, leaving them vulnerable to hacks by attackers looking to steal cars, eavesdrop on conversations, or even harm passengers by causing vehicles to crash. Several research papers also highlighted vulnerabilities including the dissemination of worms and trojans via wireless networks, onboard diagnostic ports, and CDs. To date there have been no reports of violent attacks on automobiles using a computer virus, according to SAE International. Yet, a Ford spokesman said his company had tasked its security engineers with making its Sync in-vehicle communications and entertainment system as resistant as possible to attack. Physical consequences are also among the possible risks, as one research group created a virus that can simultaneously shut off the car's lights, lock its doors, kill the engine, and

UNCLASSIFIED

UNCLASSIFIED

release or slam on the brakes. Source: <http://www.reuters.com/article/2012/08/20/us-autos-hackers-idUSBRE87J03X20120820>

DEFENSE/ INDUSTRY BASE SECTOR

Riding low and slow, Hikit targets U.S. defense contractors. Researchers at security firm Mandiant have identified a backdoor trojan, called Hikit, which has targeted a small number of defense contractors in the United States. A principal consultant at the Washington, D.C.-based company, told SCMagazine August 27 that the malware, first discovered in 2011, fell into the category of an advanced persistent threat. As opposed to financial fraud, the goal of the attackers behind Hikit is to conduct industrial espionage and steal sensitive data, he said. The trojan itself is not used to initiate a breach, but to exploit an existing server vulnerability so that attackers can maintain access to victims' data. Hikit can run commands on a targeted server, as well as transfer files to retrieve data and redirect traffic within other systems of the victims' internal network. Source: <http://www.scmagazine.com/riding-low-and-slow-hikit-targets-us-defense-contractors/article/256332/>

(Ohio) Defense contractor guilty of providing old parts to Navy. A federal jury in Ohio found a defense contractor guilty on 39 counts of fraud and related offenses for knowingly providing out-of-date electronics critical to U.S. Navy nuclear reactors, submarines, and aircraft, Stars and Stripes reported August 22. The suspect sold the Navy military surplus and decades-old parts essential to weapons systems and safety, stated the indictment filed by federal prosecutors. The convictions August 17 include 25 counts of mail fraud, 9 counts of wire fraud, 3 counts of money laundering, and 2 counts of making false official statements. A federal judge ordered the suspect to forfeit \$355,000, stated court documents August 21. The suspect sold at least 21 shipments of parts that did not conform with federal guidelines in 2006-09 through his company, J&W Technologies LLC. The non-conforming parts included transistors, semiconductors, voltage regulators, and microcircuitry. The suspect faces a maximum sentence of 20 years in prison for each fraud count, up to 10 years for the money laundering counts, and up to 5 years for each of the false official statements. Source: <http://www.stripes.com/news/us/defense-contractor-guilty-of-providing-old-parts-to-navy-1.186518>

EMERGENCY SERVICES

(New Hampshire) Inmates hack into NH prison computers. The New Hampshire State Police Major Crimes Unit responded to the department of corrections August 31 to investigate what a prison spokesperson would describe only as a —breach involving the computer system used to store and manage all correctional facility records in Concord. The former president of the union representing prison guards, said he was told by current prison guards and civilian staff that members of the major crimes unit were back at the facility August 30, along with agents from the Boston office of the FBI. He was told inmates had gained access to the prison's Corrections Information System (CORIS) that would, in theory, give them access to addresses and contact information for prison staff members, as well as sentencing and parole dates — and the ability

UNCLASSIFIED

UNCLASSIFIED

to possibly alter them. Source:

<http://www.unionleader.com/article/20120831/NEWS03/708319954>

(Louisiana) Suspects in deputy killings linked to extremists. At least some of the seven people arrested in a fatal shootout with Louisiana deputies have been linked to violent anarchists on the FBI's domestic terrorism watch lists, a sheriff said August 18. Detectives had been monitoring the group before the August 16 shootout in Laplace in which two deputies were killed and two more wounded, said the DeSoto Parish sheriff. His detectives and other law enforcement discovered the suspects were heavily armed adherents to an ideology known as the "sovereign citizens" movement. The seven suspects have been charged in the shooting of a deputy, who survived. But authorities have said murder charges are pending. Arrested were the group's apparent leader, his wife, and his two sons. Also arrested were the girlfriend of one of the sons, a man, and a woman living with him. The Gage County, Nebraska, Sheriff's Office Web site listed one of the men among its most wanted fugitives, saying he is accused of making "terroristic threats" to patrons of a Nebraska bar and law enforcement officials. Source:

<http://news.yahoo.com/suspects-deputy-killings-linked-extremists-005244499.html>

ENERGY

Ethanol plants slowed, shuttered by drought. The drought covering much of the United States is affecting ethanol plants, with a growing number either closing or cutting back on production, the Associated Press reported August 28. The plants are reacting to spiking prices or limited supplies of corn. Minnesota Public Radio (MPR) reported that at least seven ethanol plants have been idled since summer began in Nebraska, Minnesota, Indiana, Kansas, and other States. A vice president of research and analysis for the Renewable Fuels Association said most of the industry is breaking even or losing money. The idled plants include the Central Minnesota Ethanol Co-Op in Little Falls. Plant officials told MPR it does not make economic sense to keep running. It is not clear when it will re-open. Source:

<http://www.sacbee.com/2012/08/28/4764560/ethanol-plants-slowed-shuttered.html>

U.S: 78 pct. of Gulf oil production shut by storm. The U.S. government stated 78 percent of the oil production in the Gulf of Mexico has been halted in preparation for Tropical Storm Isaac, the Associated Press reported August 27. The Bureau of Safety and Environmental Enforcement reported about 1 million barrels per day of oil production has stopped as companies have evacuated 346 offshore oil and gas production platforms. That is 17 percent of daily U.S. oil production and 6 percent of consumption. The agency said 2 billion cubic feet of natural gas production is also affected. That is about 3 percent of daily U.S. production and consumption. Production was expected to quickly resume after the storm passes. Source:

http://www.dailytribune.net/news/state/article_36fae423-0724-5a5d-a580-3c0c11012d1a.html

US pipeline oversight to be toughened under proposed rules. Oversight of the U.S. pipeline system will be toughened, including a doubling of fines for mishaps, under proposed rules announced by the Department of Transportation August 17. The proposed rules, which follow a

UNCLASSIFIED

UNCLASSIFIED

number of high-profile oil leaks in the United States, are meant to implement the bipartisan pipeline safety act that Congress passed in 2011. The act authorizes the Pipeline and Hazardous Materials Safety Administration to double the maximum civil penalty to \$200,000 per violation per day. It also raises the fine for a series of related violations to \$2 million from \$1 million. The fine structure under the rule, which will be subject to a 30-day comment period, would be effective from January 3, 2012, the day the U.S. President signed the act into law. Source: <http://www.reuters.com/article/2012/08/17/usa-pipelines-rulemaking-idUSL2E8JHCVU20120817>

FOOD AND AGRICULTURE

Latest threat to drought-stricken corn: Aflatoxin. The grain industry is on high alert for a naturally occurring toxin in corn that could present a challenge to farmers hit by the worst drought in 56 years, Reuters reported August 29. Trace amounts of aflatoxin were discovered in some of the corn harvested in the United States, with a major dairy company Dean Foods in talks with State officials in Indiana and Iowa about testing milk for the carcinogenic byproduct of mold. Any major outbreak has the potential to snarl the grain handling system in the corn belt region and trigger a scramble — and price spike — for untainted corn, which will be in short supply in 2012 due to the drought. —We've actually seen it this bad before, but this year it's just a lot more widespread, said the manager of a Missouri Department of Agriculture grain inspection facility in St. Joseph. His office was testing corn samples from Kansas, Nebraska, and Iowa and finding some aflatoxin in most of them. He said most samples were sent by crop insurance adjusters who suspect a problem with the grain. Aflatoxin is the byproduct of a powdery, olive-green mold that has emerged in corn fields from Kansas through Indiana and can be fatal to livestock. The presence of the mold does not necessarily lead to aflatoxin. With the corn harvest only 6 percent complete in the United States, the world's largest corn producer and exporter, it is too soon to know whether aflatoxin will be a big problem. The U.S. Department of Agriculture's Risk Management Agency said insured farmers who suspect their fields might have aflatoxin to contact their agents before they harvest the grain to receive compensation. Source: http://articles.chicagotribune.com/2012-08-29/business/chi-latest-threat-to-droughtstricken-corn-aflatoxin-20120829_1_aflatoxin-contamination-corn-harvest-corn-samples

CDC adds 3 more deaths to toll of 2011 Listeria cantaloupe outbreak. The U.S. Centers for Disease Control and Prevention (CDC) raised the official death toll of the 2011 cantaloupe-linked Listeria outbreak from 30 to 33, Food Safety News reported August 28. Since the CDC issued its final outbreak report December 8, 2011, three more outbreak victims have died, but federal health officials had yet to confirm that these deaths were a direct result of Listeria infection. That confirmation came August 27 when CDC published an addendum to its final report, noting that —the number of outbreak-associated deaths has increased by three since December 8, 2011. Not all deaths that have occurred among outbreak victims were due to Listeria infection, noted CDC. —Ten other deaths not attributed to listeriosis occurred among persons who had been infected with an outbreak-associated subtype, said the report. —State and local public health officials reviewed causes of death listed on death certificates to

UNCLASSIFIED

UNCLASSIFIED

determine whether to attribute these deaths to listeriosis. The 2011 Listeria outbreak sickened at least 147 people. Source: <http://www.foodsafetynews.com/2012/08/cdc-adds-3-more-deaths-to-toll-of-2011-listeria-cantaloupe-outbreak/#.UDzJ9qC6TIY>

Beef cattle herds shrink amid drought. The worst U.S. drought in half a century and record feed prices have spurred farmers to shrink cattle herds to the smallest in two generations, driving beef prices higher, Bloomberg News reported August 23. Beef output will slump to a 9-year low in 2013 after drought damaged pastures from Missouri to Montana, the U.S. Department of Agriculture (USDA) estimated. The domestic herd is now the smallest since at least 1973, and retail prices reached a record in July, USDA data show. Feedlots lost \$300 a head in August fattening cattle for slaughter, after corn had surged 61 percent since June 15, University of Missouri data show. Beef output in the United States, the world's largest producer, will drop 3.9 percent to 24.58 billion pounds in 2013, the lowest since 2004, the USDA estimated. The domestic herd across ranches, feedlots, and dairies dropped to 97.8 million July 1, the smallest for the date in at least 39 years, the latest data show. The domestic price of beef will rise as much as 5 percent in 2013, more than any other food group including fruits, cereals, and dairy products, the USDA estimated. Source: <http://www.latimes.com/business/la-fi-drought-beef-20120823,0,2978935.story>

Central U.S. drought intensifies. The majority of the States of Kansas, Oklahoma, and Arkansas, as well as major portions of Nebraska and Missouri are under exceptional drought conditions, the most severe classification on the U.S. Drought Monitor, stated the August 23 update of the Monitor. Though cooler temperatures were a common feature of the weather recently, it did not stop the drought's growth; in addition to those areas under the most severe drought conditions, the majority of an area from western Nebraska to Indiana is under extreme drought. "More widespread rains in the Midwest alleviated some moderate to exceptional drought as well as abnormal dryness through southern Wisconsin, Illinois, Indiana, and Ohio and into western Kentucky again this week. Lingering drought impacts remain in many areas, leaving devastated agriculture in its wake," stated a National Oceanic and Atmospheric Administration National Climate Data Center specialist. Source: http://www.agriculture.com/news/crops/central-us-drought-intensifies_2-ar25970

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

Ex-US guard in China pleads guilty in secrets case. A former security guard at the construction site of a new U.S. consulate compound in Guangzhou, China, pleaded guilty August 30 to trying to sell secret photos and other secret information about restricted areas inside the facility to China's Ministry of State Security. According to prosecutors, he had lost nearly \$170,000 in the stock market and hoped to make \$3 million to \$5 million by selling data to the Chinese and by providing them with access to the consulate. He created a schematic that listed all security upgrades to the consulate and drew a diagram of the surveillance camera locations at the facility, according to court papers. He devised a plan in which the Chinese state security could

UNCLASSIFIED

UNCLASSIFIED

gain undetected access to a building at the U.S. consulate to install listening devices or other technical penetrations, according to his later statements to U.S. law enforcement officials. From November 2009 to August 2011, he was a civilian American guard with top secret clearance. At the behest of a U.S. law enforcement agent, he agreed to participate in a counter-surveillance project in which he was to report to his superiors any attempt by the Chinese to recruit him for intelligence purposes. He later came under suspicion by U.S. investigators. Source:

http://abcnews.go.com/International/wireStory/us-guard-china-pleads-guilty-secrets-case-17115817#.UECxs6A1_U0

Software alert claiming to be from Cyber Command aims to steal money. Fraudsters are posing as officials from U.S. Cyber Command and other federal agencies to scare Internet users into paying off bogus fines, the U.S. Computer Emergency Readiness Team warned August 28. The alert stated that it —is aware of multiple malware campaigns impersonating multiple U.S. government agencies. The malicious software pulls up a computer screen claiming that a federal agency has determined the user is involved in criminal activity. The message directs the victim to either pay a fine or lose access to the computer. The FBI has warned of similar schemes that essentially hold computers hostage until the unassuming victim pays imposter bureau agents a fine. This apparently is the first time hackers have taken the identity of the Cyber Command to collect ransom. —Affected users should not follow the payment instructions, the alert states. Source:

<http://www.nextgov.com/cybersecurity/2012/08/software-alert-claiming-be-cyber-command-aims-steal-money/57715/>

(Georgia) Copper thieves disable Ga. 400 cameras. Police were looking for thieves who disabled cameras on Georgia Highway 400 to steal thousands of dollars in copper, WSB 2 Atlanta reported August 28. The cameras are around the metro Atlanta area to help Georgia Department of Transportation (GDOT) crews monitor and respond to traffic and hazardous conditions. August 27, thieves ripped out wires from the cameras. When cameras went black on Georgia 400 at the Chattahoochee River, GDOT got suspicious and called police. Copper thieves also stole wiring from signals at the newly reopened Mitchell Street Bridge in Atlanta. Crews were not able to get the signal to operate until they replaced it. Source:

<http://www.wsbtv.com/news/news/local/copper-thieves-disable-ga-400-cameras/nRMYP/>

(Colorado) Former resident charged with taking down Colorado county computer net. A former resident who allegedly crippled Larimer County, Colorado's computer network in 2010 with a denial of service attack could now face almost 30 years in federal prison if he is convicted on all charges against him, Government Security News reported August 28. The man was indicted by a federal grand jury August 21 on charges related to a denial of service attack he allegedly implemented to retaliate against the Larimer County government. Law enforcement called the overwhelming computer attack —debilitating to the county's network. Law enforcement caught up with him at an August 23 Sonora, Texas traffic stop. The federal government wants him detained and returned to Colorado by U.S. Marshals. According to local Colorado news reports, he was allegedly angry with the Larimer County government over a drunk driving charge he received while living in the county and wanted revenge. The denial of

UNCLASSIFIED

UNCLASSIFIED

service attack was launched against the county's computer network September 22, 2010, and lasted until September 24, 2010, affecting county employees' ability to access their e-mail and the Internet, including State computer systems. The indictment alleges he intentionally damaged a protected computer, among other charges. Source:

http://www.gsnmagazine.com/node/27091?c=cyber_security

(Georgia) Prosecutor: Ga. murder case uncovers terror plot. Four U.S. Army soldiers based in southeast Georgia killed a former comrade and his girlfriend to protect an anarchist militia group they formed that stockpiled assault weapons and plotted a range of anti-government attacks, prosecutors told a judge August 27 in Ludowici, Georgia. Prosecutors said the militia group composed of active duty and former U.S. military members spent at least \$87,000 buying guns and bomb components and was serious enough to kill two people, a former soldier and his girlfriend, by shooting them in December 2011 to keep its plans secret. The group also bought land in Washington States for its activities and ultimately aimed to assassinate the U.S. President. One of the Fort Stewart soldiers charged in the case, an Army private, also gave testimony that backed up many of the assertions made by prosecutors. Prosecutors said the group called itself F.E.A.R., short for Forever Enduring Always Ready. A prosecutor said authorities did not know how many members the militia had. The four soldiers are charged by State authorities with malice murder, felony murder, criminal gang activity, aggravated assault, and using a firearm while committing a felony. A hearing was scheduled for August 30. The prosecutor said the militia group had big plans. It plotted to take over Fort Stewart by seizing its ammunition control point and talked of bombing the Forsyth Park fountain in nearby Savannah, she said. In Washington State, she added, the group plotted to bomb a dam and poison the State's apple crop. Ultimately, prosecutors said, the militia's goal was to overthrow the government and assassinate the U.S. President. Source:

http://hosted.ap.org/dynamic/stories/U/US_SOLDIERS_CHARGED_PLOT?SITE=ILNOR&SECTION=HOME&TEMPLATE=DEFAULT

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Explosion in malware bypassing traditional defenses, study shows. Advanced malware that evades signature-based detection has increased nearly 400 percent in the past year, research by security firm FireEye revealed. Companies are being hit by an average of 643 successful infections a week, according to the firm's latest Advanced Threat Report on cyber attacks that routinely bypass traditional defenses. Such defenses include intrusion prevention systems, firewalls anti-virus, and other signature, reputation, and basic behavior-based technologies. The report, which covers the first half of the year, highlights the intensified danger of email-based attacks, with researchers seeing a 56 percent growth in email-based attacks from the first to the second quarter of 2012. Another trend highlighted by the report is the increased use of dynamic, throw-away domains. Researchers saw a significant increase in dynamic links that were used five times or less. Links that were seen just once grew from 38 percent in the second half of 2011 to 46 percent in the first half of 2012. —The results of this report make it even more clear that reactive signature-based defenses cannot prevent evasive strains of malware from making their way into the enterprise, said the FireEye founder and CEO. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.computerweekly.com/news/2240162366/Explosion-in-malware-bypassing-traditional-defences-study-shows>

Cybercriminals impersonate popular security vendors, serve malware. Security researchers from Websense have intercepted a currently circulating spam campaign, impersonating popular antivirus vendors in an attempt to trick end and corporate users into downloading and executing the malicious attachment. According to Websense, the campaign is low-volume, and is currently impersonating Symantec, F-Secure, Verisign, and Sophos. The malicious payload is currently detected by 3 out of 42 antivirus scanners as Trojan.Agent Gen-Banload; TROJ_GEN.R47H1HR. Source: <http://www.zdnet.com/cybercriminals-impersonate-popular-security-vendors-serve-malware-7000003433/>

'First ever' Linux, Mac OS X-only password sniffing Trojan spotted. Security researchers have discovered a Linux and Mac OS X cross-platform trojan. Once installed on a compromised machine, Wirenet-1 opens a backdoor to a remote command server and logs key presses to capture passwords and sensitive data typed by victims. The program also grabs passwords submitted to Opera, Firefox, Chrome, and Chromium Web browsers, and credentials stored by applications including email client Thunderbird, Web suite SeaMonkey, and chat app Pidgin. The malware then attempts to upload the gathered data to a server hosted in the Netherlands. Wirenet-1 was intercepted by the Russian antivirus firm Dr Web, the same company that carried out much of the analysis of the infamous Flashback trojan. Dr Web describes Wirenet-1 as the first Linux/OSX cross-platform password-stealing trojan. Analysis work on Wirenet-1 is ongoing. Once executed, it copies itself to the user's home directory and uses AES to encrypt its communications with a server over the Internet. Source: http://www.theregister.co.uk/2012/08/29/linux_mac_trojan/

Intuit security tool spam campaign making the rounds once again. Malicious emails claiming to originate from Intuit are attempting to convince recipients they need to install a piece of software to access their QuickBooks accounts, giving them a deadline to comply. The email looks the same as an older variant that made rounds over a year ago. It seems this spam campaign has been reinitialized to steal sensitive data from Intuit customers. The message reads: —You will not be able to access your Intuit QuickBooks account without Intuit Security Tool (IST) after 31th of August, 2012. You can download Intuit Security Tool here. The links from the email currently lead to a compromised Web site from Denmark on which the cybercriminals planted a phishing Web page. The company has warned users to avoid such emails ever since the campaign started. They highlight the fact that legitimate emails will never contain —software update or —software download attachments. Source: <http://news.softpedia.com/news/Intuit-Security-Tool-Spam-Campaign-Making-the-Rounds-Once-Again-288864.shtml>

Macs at risk from 'super dangerous' Java zero-day. Hackers are exploiting a zero-day vulnerability in Java 7, security experts said August 27. The unpatched bug can be exploited through any browser running on any operating system, from Windows and Linux to OS X, that has Java installed, said the engineering manager for Metasploit, an open-source penetration

UNCLASSIFIED

UNCLASSIFIED

testing framework. The CTO of Errata Security confirmed the Metasploit exploit — which was published less than 24 hours after the bug was found — is effective against Java 7 installed on OS X Mountain Lion. He said he was able to trigger the vulnerability with the Metasploit code in Firefox 14 and Safari 6 on OS X 10.8. Although the exploits now circulating in the wild have been aimed only at Windows users, it is possible Macs could also be targeted. —What is more worrisome is the potential for this to be used by other malware developers in the near future, said antivirus vendor Intego. —Java applets have been part of the installation process for almost every malware attack on OS X this year. The engineering manager for Metasploit called the bug —super dangerous, noting that it was —totally a drive by, meaning that attackers could compromise computers simply by duping users into browsing to a Web site that hosts the attack code. Security experts have recommended that users disable Java until Oracle delivers a patch. Source:

http://www.computerworld.com/s/article/9230656/Macs_at_risk_from_super_dangerous_Java_zero_day

Cybercriminals take advantage of Android Flash Player gap on Google Play. Cybercriminals are trying to capitalize on Adobe's decision to stop distributing Android Flash Player to new users via Google Play by creating malware and adware apps that masquerade as Flash Player installers. Since August 15, Android users who did not already have Flash Player installed on their devices could no longer obtain it from Google Play. —Of course, it's possible that some Android users have missed that deadline, so they venture on to other parts of the Internet in search of alternative download sites, a communications and research analyst at GFI Software said. This is precisely what cybercriminals are counting on, as GFI's security researchers have already identified multiple SMS trojan apps packaged as Flash Player for Android. Most of these apps are distributed from third-party Russian app stores and Web sites. However, the company's researchers have also come across an English-language scam that tried to pass an adware app as Android Flash Player. —With a rooted device, future updates of this hacked app may grant or install new permissions users are not aware of, he said. Source:

http://www.computerworld.com/s/article/9230591/Cybercriminals_take_advantage_of_Android_Flash_Player_gap_on_Google_Play

Dropbox upgrades security with two-factor authentication. The file-sharing utility Dropbox is now offering two-factor authentication. Dropbox said in July it planned on introducing two-factor authentication after user names and passwords were stolen from another Web site and used to access accounts. Users first must upgrade their client to version 1.5.12. Users can opt to receive the six-digit code sent by SMS to their mobile phone when a new device is used to access their account. A valid code can also be obtained by using an application that supports the Time-Based One-Time Password protocol, such as Google Authenticator, Amazon AWS MFA, or Authenticator, according to Dropbox. Apple users can opt to generate a code from the terminal application using the OATH tool, Dropbox said. While setting up two-factor authentication, users get a 16-digit backup code that can be used to unlock their account if they lose their phones and cannot obtain codes through SMS or an application. Dropbox is also working on a feature for users to —untrust their current browser or all other browsers, which would mean that a code would be required upon the next attempted login. Source:

UNCLASSIFIED

UNCLASSIFIED

http://www.computerworld.com/s/article/9230619/Dropbox_upgrades_security_with_two_factor_authentication

Trend Micro security expert: Malware attack against VMware limited in scope. Security researchers determined that some new variants of a new malware family called “Crisis,” aka “Morcut,” can infect VMware virtual machines and Windows Mobile devices. But, a security expert at Trend Micro points to current evidence that says the majority of VMware’s most widely deployed products are not currently under attack. “VMware has a family of test development and productivity products called Workstation and Player,” said the director of datacenter products at Trend Micro, in an interview with CRN. “This malware only affects these types of hypervisors. The data center products are not under attack at this point. But, it’s important to be aware that some malware writer in the future can try to leverage this same technique against the data center products. So, it’s important to make sure that your anti-malware products are up to date and that you have effectively locked down access to key directories and repositories.” He said at this point, it appears that the malware in question is aimed at spying upon the users, most likely Web behavior and communications. The rate of incidence in the wild appears to be very low, at this point, with fewer than 100 systems impacted, according to Trend Micro. Source:

<http://www.crn.com/news/security/240006175/trend-micro-security-expert-malware-attack-against-vmware-limited-in-scope.htm>

WebSense Security Labs discusses malware targeting BlackBerry users. WebSense Security Labs researchers have intercepted a malware campaign aimed at BlackBerry users. The campaign runs through fake emails stating the recipient has successfully created a BlackBerry ID. The email says that to enjoy the full benefits of the BlackBerry ID, the recipient should follow the instructions given in the attached file. This is done to trick the user into running the malicious file. The fake email is a copy of a genuine email from BlackBerry. Websense researchers found that once the attachment is set running, it drops other executable files and modifies the system registry. The malware programs automatically start, once the system restarts. Source: <http://tech2.in.com/news/general/websense-security-labs-discusses-malware-targeting-blackberry-users/390882>

NATIONAL MONUMENTS AND ICONS

(California) Two more Yosemite visitors stricken with deadly virus. Two more visitors to Yosemite National Park were diagnosed with a deadly rodent-borne virus, raising the total number of people infected in the unusual outbreak to six, California public health officials said August 30. Two of the six infected died from hantavirus pulmonary syndrome. Most of the victims are believed to have contracted the virus while staying in tent-style cabins this summer in the Curry Village camping area. Park officials the week of August 27 shut down 91 insulated tent-cabins after finding deer mice, which carry the disease and can burrow through pencil-sized holes, nesting between the double walls of the structures. Park authorities notified 2,900 parties of visitors who rented the tent cabins from June through August that they may have been exposed to hantavirus. Experts continued to investigate the outbreak, and the number of

UNCLASSIFIED

UNCLASSIFIED

cases could rise as visitors who were exposed to the virus but have not yet shown symptoms fall ill, the agency said. Hantavirus is carried in rodent feces, urine and saliva that dries out and mixes with dust that can be inhaled by humans, especially in small, confined spaces with poor ventilation. People also can be infected by eating contaminated food, touching contaminated surfaces or being bitten by infected rodents. The virus starts out causing flu-like symptoms, including headache, fever, muscle ache, shortness of breath, and cough. Initial symptoms may appear up to 6 weeks after exposure and can lead to severe breathing difficulties and death.

Source: http://articles.chicagotribune.com/2012-08-30/news/sns-rt-us-usa-hantavirus-yosemitebre87u04p-20120830_1_curry-village-tent-cabins-rodent-borne-virus

(Alaska) Site of deadly bear mauling remains closed. About 200 square miles of Alaska backcountry terrain where a California hiker was mauled to death by a grizzly bear remained closed August 26 as investigators continued to piece together what happened. Rangers at Denali National Park were planning to recreate the steps taken by the San Diego man before he was attacked August 24 near the Toklat River, park officials said. Before the attack, the man photographed the male bear for at least 8 minutes from a distance of 50 to 100 yards. A State trooper fatally shot the bear August 25. A park spokeswoman said park pilots would fly over the area to look for other backpackers believed to still be in the general vicinity or heading in that direction. A park spokeswoman said rangers might also go on foot to alert — not evacuate — the party believed to still be there. The hiker's remains were recovered August 25 and were sent to the State medical examiner's office in Anchorage. Denali is 240 miles north of Anchorage, and spans more than 6 million acres. Source:

<http://www.sfgate.com/news/article/Site-of-deadly-bear-mauling-remains-closed-3816598.php>

(Idaho) Wildfire forces evacuations near Salmon River. About two-dozen homes and properties north of the Salmon River Road were ordered to evacuate due to the 99,000-acre Mustang Complex Fire west of North Fork, Idaho, KTVB 7 Boise reported August 24. The Mustang Complex Fire includes several smaller fires burning in Idaho's Salmon-Challis National Forest. The Lemhi County Sheriff's Office issued a mandatory evacuation order for the Indian Creek and Spring Creek drainage areas August 23. Source:

<http://www.ktvb.com/news/Wildfire-forces-evacuations-near-Salmon-River--167320705.html>

POSTAL AND SHIPPING

Beware the new USPS email scam. An old email scam involving fake shipping service emails that include outright financial threats against the recipient has surfaced again, Examiner.com reported August 29. These emails may be used to install a virus on a computer or to collect data that will be used in Internet fraud or identity theft. The threat being circulated said — Unfortunately, we failed to deliver the postal package you have sent on the 27th of August in time, because the recipient's address is erroneous. Please go to the nearest UPS office and show your shipping label. The email includes a submit button that, supposedly, will print a shipping label. The email is not from the U.S. Postal Service. So far, USPS.com includes no information about this latest email scam. When the email recipient clicks the button to print

UNCLASSIFIED

UNCLASSIFIED

the shipping label, the page transfers to a failure page on a site run by comicgenesis(dot)com, which may also be a victim in this latest scam. Snopes(dot)com has reports on file for a package delivery virus from April of this year, March 2011, July 2008, and August 2008. The recurring entries point out that a package delivery email is a popular delivery choice for emailed viruses and malware. Source: <http://www.examiner.com/article/beware-the-new-ups-email-scam>

(Oregon) Man charged with threatening to blow up Eugene post office. Federal authorities have filed charges against a man accused of using a phone to call in a bomb threat against a U.S. post office in Eugene, Oregon, which triggered the evacuation of nearby buildings. The U.S. attorney's office in Eugene charged the suspect by criminal information, a document typically filed in advance of a guilty plea. The papers were made public August 29. The suspect was accused of parking a van outside the post office November 16, 2010, where he allegedly phoned a bomb threat to authorities. Police evacuated nearby buildings and shut down three avenues. Eugene police negotiators talked the suspect out of the van. Authorities found no explosives inside. Source: http://www.oregonlive.com/pacific-northwest-news/index.ssf/2012/08/man_charged_with_threatening_t.html#incart_river_default

PUBLIC HEALTH

Damage from healthcare data breaches spreading. Almost twice as many people were affected by healthcare data breaches in 2011 as in 2010, according to a report released August 29. The total number of breaches dropped by 32 percent to 145 but the number of people affected by those breaches doubled to 10.8 million. The latest tally included the loss of a single back-up tape containing 5 million records. The findings were based on a review of breaches reported to have occurred in 2011 according to the Department of Health and Human Services' Web site. The self reporting of breaches is a requirement for businesses under the Health Information Technology for Economic and Clinical Health Act (HITECH). The data shows California had the highest number of breaches in 2011 with 15, followed by Texas (11), Illinois (8), Florida (7), and New Jersey (7). Breaches that involved the loss of healthcare data affected the most individuals — 6.1 million. Theft affected 2.4 million, unknown cause affected 1.9 million, and loss affected 1.2 million. Unauthorized access, hacking, improper disposal and other combined affected about 464,000 individuals. Access to portable electronic devices such as thumb drives, backup tapes, CDs, DVDs, and X-Ray films accounted for 28 percent of the breaches and affected 8.2 million people. Paper and laptops account for 27 percent and 22 percent of the breaches, respectively, but combined accounted for only 5 percent of the individuals affected by breaches. Source: <http://www.healthleadersmedia.com/print/TEC-283933/Damage-from-Healthcare-Data-Breaches-Spreading>

66 West Nile deaths so far in 2012; more expected. A total of 1,590 cases of West Nile virus, including 66 deaths, have been reported through late August in the United States, the highest human toll by that point in the calendar since the mosquito-borne disease was first detected in the country in 1999, health officials said August 29. In hard-hit Texas, the number of confirmed cases soared to 894, with 34 people dead, according to the Texas Department of State Health Services. All 48 contiguous States have reported cases of West Nile virus in birds, which act as

UNCLASSIFIED

UNCLASSIFIED

hosts; in mosquitoes, which transmit it by biting birds and then mammals including humans, or in people. Only Alaska and Hawaii have been spared. And 43 States have at least one human case. Source: http://www.dispatch.com/content/stories/national_world/2012/08/30/66-west-nile-deaths-so-far-in-2012-more-expected.html

Salmonella strain linked to multistate outbreak found at cantaloupe farm. The strain of Salmonella that has now sickened 178 people in 21 States has been found on samples of cantaloupes from the southwestern Indiana farm previously suspected to be the source of the bacteria, confirming the link between the grower and the ongoing outbreak, Food Safety News reported August 28. The week of August 20, the U.S. Food and Drug Administration announced that Chamberlain Farms was the likely site of contamination, but at the time test results had not confirmed the connection. The agency collected samples at the Owensville, Indiana farm between August 14-16, and announced August 28 that —samples of cantaloupe taken from the farm have shown the presence of Salmonella Typhimurium with a DNA fingerprint that matches the outbreak strain. Source: <http://www.foodsafetynews.com/2012/08/strain-causing-salmonella-outbreak-found-at-cantaloupe-farm/#.UD4iH6C6TIY>

(Kansas) 19 West Nile cases, 1 death reported in Kansas. Kansas has its first reported death of 2012 from the West Nile virus amid an unusual spike in cases nationwide, State health officials said August 24. The State Department of Health and Environment reported that the State has had 19 probable or confirmed cases of the mosquito-borne virus so far this year. Typically, most cases are reported in August and September. Source: <http://www.sfgate.com/news/article/19-West-Nile-cases-1-death-reported-in-Kansas-3813863.php>

TRANSPORTATION

Drones being used to track hurricanes. Federal hurricane trackers will start experimenting with unmanned boats and aircrafts to learn more about how to anticipate and track the movements of hurricanes, Homeland Security News Wire reported August 31. The National Aeronautics and Space Administration (NASA) and the National Oceanic and Atmospheric Administration (NOAA) are teaming up and using a pair of military-surplus Global Hawk spy drones, which are known more for spying on battlefields than chasing storms. The National Journal reported that drones are not being used in the tracking of Hurricane Isaac, but officials expect to have the program up and running at the height of hurricane season. The first of the two drones is expected to touch down at NASA's Wallops Flight Facility in Virginia with a preliminary flight to take place soon after. Officials hope to get the drones prepared for a first test in mid-September. Source: <http://www.homelandsecuritynewswire.com/dr20120831-drones-being-used-to-track-hurricanes>

(Texas) Man accused of bomb threat to SA Airport. San Antonio police arrested a man accused of making a bomb threat at the San Antonio International Airport, the San Antonio Express-News reported August 24. While not accused in the August 1 threat that shut down the facility, he faces one count of making a threat or influencing the activities of a branch of the federal government in connection with a phone call he allegedly made August 22. He was being held in

UNCLASSIFIED

UNCLASSIFIED

a county jail on \$30,000 bail. Source:

http://www.mysanantonio.com/news/local_news/article/Man-accused-of-bomb-threat-to-SA-Airport-3812383.php#ixzz24TDaISiS

WATER AND DAMS

(Pennsylvania) Fear of security breach prompted tap water ban; probe ongoing. Pennsylvania State Police were investigating a possible security breach at the Shoemakersville water plant that caused officials to warn residents of the borough and Perry Township not to drink the tap water, the borough emergency management coordinator said August 28. The drinking ban went into effect August 24 and was lifted August 27 after a series of tests by the State Department of Environmental Protection and an independent testing firm determined the water met all safety levels for consumption. The steps officials took to warn residents not to drink the water were only a precaution. New security measures were implemented at the plant following the incident. Clean water was made available to residents while the ban was in place. Source:

<http://readingeagle.com/article.aspx?id=412015>

(Tennessee) Tennessee Valley Authority liable for 2008 coal ash spill-ruling. The Tennessee Valley Authority (TVA) is legally responsible for a 2008 accident that sent 5 million cubic yards of toxic coal sludge oozing into a small community in eastern Tennessee, a federal judge ruled August 23. The judge said the levee that was supposed to keep the wet coal ash confined failed because of conduct on the part of the authority. As a result, the federally owned utility will have to pay unspecified damages to more than 800 plaintiffs who sued after the spill. Hundreds of acres of land in Roane County were covered and hundreds of residents were forced from their homes. "Had TVA followed its own mandatory policies, procedures, and practices, the subsurface issues underlying the failure of North Dike would have been investigated, addressed, and potentially remedied before the catastrophic failure," the judge wrote. The TVA said in a statement that it had already purchased nearly 180 properties affected by the spill, settled more than 200 other claims submitted by residents, and paid \$43 million to the Roane County Economic Development Foundation for use by communities in the affected area. The ruling signals the beginning of a new phase in litigation against the TVA; plaintiffs will now have to prove they were each directly impacted by the spill. Source:

<http://www.reuters.com/article/2012/08/24/us-usa-environment-tva-spill-idUSBRE87N00120120824>

HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center: 866-885-8295 (IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455;**

UNCLASSIFIED

UNCLASSIFIED

US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED