

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

UNCLASSIFIED

NORTH DAKOTA

White Rock Dam outflows cut because of heavy rain. The U.S. Army Corps of Engineers in St. Paul District, cut outflow to zero at White Rock Dam August 1 due to rain July 31. White Rock Dam is part of the Corps' Lake Traverse project in Wheaton, Minnesota. The Lake Traverse project is operated to keep Wahpeton, North Dakota, below a flood stage of 10 feet during the summer. Due to higher than average spring runoff and continued summer rains, Lake Traverse is 2.5 feet higher than normal and Mud Lake, also part of the Lake Traverse project, is 6.5 feet higher than normal. Lake levels are expected to rise in both lakes. Lake Traverse is at elevation 978.9 feet, and is forecaste to climb more than half a foot by early the week of August 8 barring additional rain. Source: <http://www.valleynewslive.com/story/15196969/white-rock-dam-releases-stopped-du>

Too Much Rain. The U.S. Army Corps of Engineers reported that wet weather in the North Dakota region forced them to increase outflows at Bald Hill Dam near Valley City to 4,000 cubic feet per second (cfs) August 1. As a result, levels at Lake Ashtabula were 4 feet higher than normal this time of year. "They never released more than 5,000 cfs from the dam until 2 years ago," said one resident. The Corps said the Sheyenne River could rise 16 feet by August 2. With more rain on its way, there was a chance more water could be released. Source: <http://www.valleynewslive.com/story/15190432/more-releases>

Corps sets Missouri Basin flood storage plan for fall and winter. The U.S. Army Corps of Engineers was still sending above-normal releases from its six Missouri River dams in early August, and it did not plan to increase its flood storage capacity this fall and winter due to flooding risks at downstream levees. The commander of the Corps' Northwest Division, said the planned release schedule, announced July 29, will allow the Corps to get systems ready for the 2012 season when it starts March 1. Several factors influenced the decision, including: peoples' need to return to flooded homes, farms and businesses; weather forecasts for this fall and winter; risks from continued high water on saturated levees; the need to inspect and repair dams and damaged infrastructure, and the need to release water in Kansas reservoirs. Record snowfall and rain in May created runoff that peaked at 72.8 million acre-feet (MAF) in a system designed to handle 40 MAF, the commander said. At Gavins Point Dam, near Yankton, South Dakota, the release dropped from a record 160,000 cubic ft per second (cfs) — a rate held since June 24 — to 155,000 cfs July 30 and 150,000 cfs August 1. It will fall to 40,000 cfs September 30, and 20,000 cfs December 1. The other dams, all upstream, also started reducing releases. The commander added the risk to levees continues as long as water is high. Source: http://enr.construction.com/infrastructure/water_dams/2011/0802-corpssetsmissouribasinfloodstorageplanforfallandwinter.asp

REGIONAL

(Nebraska; Iowa; South Dakota) USGS trolls Missouri River with side-scan sonar looking for bridge damage. The U.S. Army Corps of Engineers banned all recreational watercraft from the Missouri River and its backwaters since early July due to dangerous conditions. The river is filled

UNCLASSIFIED

UNCLASSIFIED

with downed trees, jetties, and submerged debris that can quickly punch a hole into a hull. So, when the U.S. Geological Survey launches its 18-foot steel boat on the river, it's got to be for a good reason. A U.S. Geological Survey (USGS) crew that has been plying the Missouri River since the flood began — checking out bridge piers and pipelines for the Corps, the U.S.

Environmental Protection Agency, and the road departments in Nebraska and Iowa — hit the water again August 2 near Nebraska City, Nebraska. Using sonar, the crew bounces sound waves off the bottom of the river to create an intense digital image of the water's scouring effect on the channel and bridge piers. It is the same high technology that is used to find sunken shipwrecks. There is cause for concern. On June 27, authorities closed the Decatur bridge because of fears scouring had eroded some of the approach on the Iowa side of the river. Scouring as deep as 50 feet was found along bridge piers. The bridges to be inspected are in Vermillion, South Dakota, Yankton, South Dakota, Rulo, Nebraska City, Plattsmouth, Bellevue, South Omaha, Nebraska, Interstates 80, 480, and 680, Blair, Decatur, and two are in South Sioux City. The Chief Standing Bear Memorial Bridge near the village of Niobrara is the other. Source: http://journalstar.com/news/state-and-regional/nebraska/article_42692364-e382-5467-82c7-77987dcc196d.html

(South Dakota) Flood cleanup on the horizon in SD capital of Pierre; likely to begin late this month. Officials in Pierre plan to launch a significant flood cleanup in the South Dakota capital 3 days after the Missouri River falls back within its banks. The U.S. Army Corps of Engineers plans to reduce releases from the Oahe Dam north of Pierre, to 85,000 cubic feet per second (cfs) August 24, to put the bloated river back in its banks. Releases this summer have reached levels nearly double that amount because of heavy spring snowmelt and rain. The flood cleanup effort will include unplugging storm sewers and removing sump pumps being used to pump rainwater from areas behind dikes. Starting August 5, officials plan to start removing barricades and access checkpoints that have guarded Pierre neighborhoods most in danger of flooding. Source: <http://www.therepublic.com/view/story/e8356985769248c4a954bd23d4eac79b/SD--SD-Flooding-Pierre/>

(South Dakota) Northeast South Dakota dam in need of repair. Officials used pumps to lower the level of White Lake in northeast South Dakota, August 2 so repairs could be made to a damaged dam. The state game, fish, and parks department reported a chunk of concrete fell from the spillway at the dam northeast of Britton after heavy rains. Officials waited until water stopped going over the spillway before beginning repairs to ensure the dam did not sustain any more damage. Source: http://rapidcityjournal.com/news/state-and-regional/northeast-south-dakota-dam-in-need-of-repair/article_7a00c303-98f9-5616-bd0e-c06eac2f6ff2.html

(Wyoming; Montana) Midwest flooding slowed trains, Wyo. coal exports. Flooding in the Midwest slowed down coal trains and reduced exports from the mines of at least one coal company operating in the Powder River Basin. Cloud Peak Energy said it delivered 1 million fewer tons of coal in the second quarter of 2011 compared to the second quarter of 2010. The Gillette News-Record reports the company expects flooding to continue to affect railways into September. The Cloud Peak president and CEO said he expects production in 2011 to remain

UNCLASSIFIED

UNCLASSIFIED

within his earlier projection of 93 to 96 million tons. Cloud Peak is based in Gillette, Wyoming, and operates three mines in the basin: the Cordero Rojo Mine in Campbell County, Antelope Mine in Converse County, and Spring Creek Mine in Montana. Source:

<http://www.greenwichtime.com/news/article/Midwest-flooding-slowed-trains-Wyo-coal-exports-1719663.php>

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Narco sub with 7.5 tons of cocaine caught in Caribbean. The U.S. Coast Guard (USCG) caught a narco submarine trying to smuggle \$180 million worth of cocaine into the United States, intercepting the drug vessel as the sub's own crew tried to sink her off the coast of Honduras. USCG video shows the crew of the semi-submersible craft jumping off the boat and into a yellow life raft. As a USCG boat comes alongside, the submarine can be seen quickly sinking into the Caribbean Sea. An FBI dive team later recovered 7.5 tons of cocaine from the boat. The interdiction was the first in the Western Caribbean; according to the USCG, submarines are regularly used to move contraband in the Eastern Pacific. Drug traffickers design the vessels so they can be sunk rapidly when threatened by law enforcement. The USCG began searching for the sub when it sank July 13, and was assisted by several other cutters and the Honduran Navy, but did not locate its underwater resting place until July 26. The sub had been spotted July 13 by a fixed wing aircraft, which then alerted the U.S. Customs and Border Protection (CBP). The crew of a CBP patrol plane found the ship and then alerted the USCG. The USCG took the sub crew into custody after the interception, and then handed them off to authorities on shore. The case is under investigation. Source: <http://abcnews.go.com/Blotter/narco-75-tons-cocaine-caught-caribbean/story?id=14205749>

Iran rips-and-replaces centrifuges post-Stuxnet. A new report suggests Iran's nuclear program has not recovered from the Stuxnet worm as previously believed. It appears Iran is still replacing thousands of expensive centrifuges that were damaged by the worm. Stuxnet was not entirely purged from Iran's nuclear facilities and it resurfaced again to damage more systems, "Western intelligence sources" told DEBKAFfile July 20. DEBKAFfile claimed Iran had replaced an estimated 5,000 centrifuges to remove the threat. "Iran finally resorted to the only sure-fire cure, scrapping all the tainted machines and replacing them with new ones," according to the report, noting a spokesperson from Iran's foreign ministry said July 19 it was installing newer and faster centrifuges at its nuclear plants to speed up operations. The worm was among the most sophisticated pieces of malware ever discovered in the wild. It exploited the AutoRun functionality on Windows to infect computers from USB drives. It then used a hardcoded default password for Siemens management applications to compromise the machine before taking over specialized industrial-control computers that ran a proprietary operating system from Siemens. The worm also hijacked the facility's monitoring system to falsely show the machines were functioning normally, preventing officials from catching on to what was really

UNCLASSIFIED

UNCLASSIFIED

happening. While Stuxnet specifically targeted Siemens industrial process control computers used in nuclear centrifuge operations, an ESET researcher noted there are "plenty other" industrial process automation and control systems being used on "modern critical infrastructure", and that network operators have to assess their threat exposure level and how to mitigate it. Source: [http://securitywatch.eweek.com/scada/iran_rip-and-replaces-centrifuges-post-stuxnet.html?kc=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+RSS/security_watch+\(eWEEK+Security+Watch+Blog\)](http://securitywatch.eweek.com/scada/iran_rip-and-replaces-centrifuges-post-stuxnet.html?kc=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+RSS/security_watch+(eWEEK+Security+Watch+Blog))

BANKING AND FINANCE INDUSTRY

Daphne-born terror suspect placed on U.S. Treasury blacklist. The U.S. Treasury Department July 29 placed a Daphne, Alabama native on a terrorist blacklist to freeze any assets connected with him in the United States and lock him out of the U.S. financial system. The man attended Daphne High and the University of South Alabama before joining the terrorist group al-Shabaab in Somalia. The Office of Foreign Assets Control (OFAC) issued a notice July 29 naming the man and another member of the Somali group to that office's list of "specially designated nationals." The assets of those on the list are blocked and U.S. citizens are prohibited from dealing with them financially. The Alabama native has been linked to recruiting and fundraising activities for al-Shabaab in the United States, Canada, and elsewhere, according to published reports. In the background material published on the Treasury Department's Web site, he is described as "one of al-Shabaab's key figures." The material further states that: "[He] serves as a military tactician, recruitment strategist and financial manager for al-Shabaab. [He] has commanded guerilla forces in combat, organized attacks and plotted strategy with al-Qa'ida. He was also involved in organizing a suicide bombing attack carried out by a Somali-American from Minnesota who traveled to Somalia to join al-Shabaab. That attack, and four others organized by [the man] and carried out in October 2008, killed more than 20 people." Source: <http://blog.al.com/live/2011/07/daphne-born-terrorist-placed-o.html>

Fake 'wrong transaction' hotel spam hits e-mail. Hundreds of e-mails have been making the rounds in the past few days informing people a hotel made a "wrong transaction" while processing their credit card. In turn, the e-mails offer recipients a refund. The director of research in computer forensics at the University of Alabama at Birmingham (UAB) wrote he has spotted 434 slight variants of the scam, with subject titles such as "Hotel Renaissance Chicago made wrong transaction", "Hotel Hilton Las Vegas made wrong transaction", and "Wrong transaction from your credit card in Hilton Atlanta." To receive the refund from the erroneously charged credit card, victims are told to fill out a form attached to the e-mail. As with nearly all e-mail scams, the attached form is where the danger lies. In this case, the malicious file is masked as an executable download called RefundForm(dot)exe, but it's actually a Trojan that installs fake anti-virus software on victims' computers that they are then pressured into paying for. The UAB researcher said the hotel spam messages all appear to be originating from the same botnet of computers that recently spread the "overdue credit card" scam. Source: http://www.msnbc.msn.com/id/43948767/ns/technology_and_science-security/

UNCLASSIFIED

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Report rips chemical testing program. A federal program that relied on companies volunteering information on the potential health risks to children from chemicals released into the environment or found in everyday consumer products was declared a failure in a report by the U.S. Environmental Protection Agency's Inspector General. The failure of the Voluntary Children's Chemical Evaluation Program, started in 2000, leaves the public without a reliable source of information about such exposure, said the report. The Inspector General said the EPA neglected to review chemicals that pose the greatest risk to children, and did not use its regulatory power to compel industry to participate in the voluntary program. The EPA, in a letter responding to the report, released last month, said it concurred with the overall finding that the program "did not achieve its goals to design a process to assess and report on the safety of chemicals to children." The agency said an "enhanced chemicals management" program started in 2009 would address the impact of chemicals on children. Source: http://online.wsj.com/article/SB10001424053111903885604576486622748559028.html?mod=googlenews_wsj

EPA publishes rule to improve reporting of chemical information. The U.S. Environmental Protection Agency (EPA) issued a new rule August 2 to increase the type and amount of data it collects on commercial chemicals from chemical manufacturers, allowing it to better identify and manage potential risks. The improved rule, known as the Chemical Data Reporting Rule (CDR), also requires that firms submit data electronically, rather than on paper, and limits confidentiality claims by companies. The changes are part of the EPA Administrator's commitment to strengthen the agency's chemical management program, and increase the transparency of critical information on chemicals. The CDR Rule, which falls under the Toxic Substances Control Act Inventory Update Rule (IUR), requires more frequent reporting of critical data on chemicals, and requires the submission of new and updated data relating to potential chemical exposures, current production volume, manufacturing site-related data, and processing and use-related data for a larger number of chemicals. The EPA is requiring companies to submit the data through the Internet, using the agency's electronic reporting tool. Companies will be required to start following the new reporting rules in the next data submission period, which will occur February 1, 2012 to June 30, 2012. Source: <http://yosemite.epa.gov/opa/admpress.nsf/0/346b93365e96c25e852578e000542b73?OpenDocument>

Highest levels of radiation since March 11 detected at Fukushima nuclear reactors. Tokyo Electric Power Co. (TEPCO) said August 1 it had detected radiation doses exceeding 10 sieverts per hour, the highest level of radiation measured since the outbreak of the crisis at the Fukushima No. 1 Nuclear Power Plant in Japan, outside the buildings for two reactors — a new discovery that could hamper efforts to bring the troubled reactors under control. The dosage, which exceeded the capacity of measuring equipment, was detected near the surface of an exhaust pipe between the No. 1 and 2 reactors at the Fukushima nuclear complex, TEPCO said. The high levels of radiation mean a person could be exposed to 250 millisieverts of radiation — the upper limit set by the government for workers engaged in restoration work at the

UNCLASSIFIED

Fukushima plant — within 90 seconds. The utility firm said it had made the area within a radius of several meters from the trouble spot off-limits, and that it was going to shield the area. TEPCO said the radiation doses would not affect restoration work. But if similar doses were found elsewhere on the premises of the nuclear plant, it could affect efforts to bring the nuclear reactors under control. The exhaust pipe where the radiation doses were detected is used in the event of an emergency to release gas from reactor containment vessels. Steam containing high levels of radioactive substances may have remained in the pipe after TEPCO vented steam from the No. 1 reactor March 12 in an attempt to protect the reactor containment vessel. Radioactive particles may have also adhered to the outside of the pipe. Source: <http://mdn.mainichi.jp/mdnnews/news/20110802p2a00m0na018000c.html>

Radioactive waste worries local governments/Officials seek guidance from central authorities on how to permanently dispose of sludge, ash. Many local governments in Japan are troubled over how to handle waste containing radioactive cesium, including sludge discharged from water and sewage treatment plants, and ash. According to surveys by the health, labor and welfare Ministry and The Yomiuri Shimbun, more than 120,000 tons of such radioactive waste is being stored in Tokyo and 13 prefectures in the Tohoku and Kanto regions. Sludge is discharged when river water and sewage is purified at treatment plants — water treatment plants discharge sludge containing mostly earth and sand, while sludge from sewage treatment plants contains domestic wastewater and excrement. The government presented a preliminary guideline for handling such radioactive waste in June. It asked local governments to take measures to block radiation rays if radioactivity exceeds 100,000 becquerels, but it does not give directions as to final disposal methods. The guideline stipulates that if the radioactivity is less than 100,000 becquerels, waste can be temporarily stored at so-called controlled landfill sites, at which hazardous substances will not leak into soil. But little progress has been made in securing such disposal sites to accommodate radioactive waste. For example, the Gunma prefectural government, which lacks a disposal site sufficiently far from residential areas, has consulted with 23 municipalities from which sludge and ash are brought to the plant. It is considering returning radioactive waste to sewage treatment sites or private-sector garbage disposal sites in the municipalities for storage. Source: <http://www.yomiuri.co.jp/dy/national/T110731002780.htm>

COMMERCIAL FACILITIES

(New Hampshire) Londonderry YMCA camp evacuated after man with assault rifle spotted nearby. A YMCA camp in Londonderry, New Hampshire, was evacuated August 2 after a man wearing camouflage was seen stalking through the woods carrying a firearm that witnesses described as resembling an assault rifle. The man was seen walking toward children playing behind the camp, witnesses reported. Local police responded to the camp about 11:30 a.m. Police quickly established a perimeter around the camp while the patrol sergeant coordinated a search of the woods. About 200 children and counselors were evacuated from the camp, and the building locked, police said. The area searched is riddled with hiking trails and a well traveled railroad bed, police said. Two search teams were out for over an hour, but the subject of the search was not found, police said. A New Hampshire State Police K-9 officer, along with a

UNCLASSIFIED

UNCLASSIFIED

Londonderry police cover team, searched the area for about 45 minutes and were not able to establish a track or find the subject. Source: <http://www.nashuatelegraph.com/news/928058-196/ymca-camp-evacuated-after-man-with-assault.html>

(Ohio) Shooting kills one, injures three after George Clinton concert at Luke Easter Park in Cleveland. Four people — two boys, a man and a woman — were shot July 30 at about 10 p.m. at Luke Easter Park in Cleveland, Ohio, during the eighth annual Unity in the Park festival. A 16 year-old male victim died July 31, and the rest of the wounded were being treated at MetroHealth Medical Center, a police sergeant said. A spokeswoman at Cleveland's Emergency Medical Services reported one of the victims was in critical condition. Two others were stable. Authorities said they were searching for a male suspect who pulled out a handgun and fired into a group of people during the fight. No arrests were reported in the hours after the shooting, the police sergeant told the Associated Press. "It was a large fight. Somebody in the crowd produced a handgun and fired several - 20 - times," the police sergeant said, adding all four victims were hit by gunfire. The 16-year-old who died was shot in the head, and a 20-year-old woman suffered a gunshot wound to the neck, police said. A police statement added that a 14-year-old boy and a 23-year-old man also were hospitalized — each with a gunshot wound in the left leg. It wasn't immediately clear how long after musicians had performed that the shooting erupted — nor how many people were still in the area. Police do not have a description of the shooter. Thousands of residents, many from the Mount Pleasant and Kinsman neighborhoods, gathered at the park earlier in the day for the celebration, aimed at strengthening the community and family. Source: http://blog.cleveland.com/metro/2011/07/shooting_at_luke_easter_park_.html

COMMUNICATIONS SECTOR

(Kansas) Copper thieves strike AT&T phone line in N. Wichita. Police in Wichita, Kansas, are looking for thieves who stole around \$6,000 worth of copper wire from an AT&T site. It happened some time between July 31 and August 1 in the 2400 block of W. 29th Street North. Police said thieves stole 65 feet of copper wire, wiping out telephone and data in that area. The Sedgwick County Law Enforcement Training Center is among those that lost telephone lines and Internet service, but it has since been restored. Source: http://articles.kwch.com/2011-08-03/at-t-site_29848413

FCC announces major spectrum-sharing agreements with Canada and Mexico enabling 4G wireless broadband and public safety communications in the border areas. The Federal Communications Commission (FCC) announced August 1 it has reached arrangements with Industry Canada and Mexico's Secretariat of Communications and Transportation (SCT) for sharing commercial wireless broadband spectrum in the 700 MHz band along the U.S.-Canadian and U.S.-Mexican border areas. The FCC also reached an arrangement with Industry Canada for sharing spectrum in the 800 MHz band. These actions will help support commercial broadband services and public safety mission-critical voice communications. The technical sharing principles reached on 800 MHz will pave the way for completion of 800 MHz rebanding by U.S. public safety and commercial licensees operating along the U.S.-Canadian border. The FCC

UNCLASSIFIED

UNCLASSIFIED

ordered rebanding to alleviate interference to public safety licensees in the band caused by commercial cellular licensees. The arrangement specifies (1) how primary channels will be allotted between the United States and Canada, (2) the technical parameters for operation on these channels within 140 kilometers (87 miles) of the common border, and (3) a schedule for transitioning facilities from the channels needed by the United States to complete rebanding along the U.S.-Canadian border. Source: <http://www.fcc.gov/document/fcc-announces-major-spectrum-sharing-agreements-canada-and-mexico-enabling-4g-wireless-broa>

CRITICAL MANUFACTURING

Cloud Engines recalls Pogoplug video file sharing device due to fire hazard. The U.S. Consumer Product Safety Commission and Health Canada, in cooperation with Cloud Engines Inc., August 2 announced a voluntary recall of 11,000 Pogoplug Video file sharing devices. Consumers should stop using recalled products immediately unless otherwise instructed. The unit can overheat or catch fire, emitting excessive heat, sparks, smoke, or flames. Cloud Engines has received three reports of the units overheating. One device caught fire, one device emitted smoke, and one device melted, damaging the desk it was on. The device is a black desktop electronics box, measuring about 2.5 inches wide, 7 inches deep, and 5.5 inches high. It is used to stream and share videos, photos, and music and to provide remote access to files stored on drives attached to the device. The device has the word "Pogoplug" on the side. "Model: Pogoplug Video" is listed on a label on the bottom of the device. The devices were sold at Adorama, B&H, Best Buy, Buy.com, J&R, Pogoplug.com, New Egg, and Sony Style from March 2011 through June 2011. Consumers should immediately stop using and unplug the devices and contact Cloud Engines to receive a refund or replacement device. Source: <http://www.cpsc.gov/cpscpub/prerel/prhtml11/11294.html>

NexTorch recalls flashlight batteries due to fire hazard. The U.S. Consumer Product Safety Commission, in cooperation with NexTorch Inc., August 3 announced a voluntary recall of 16,000 NexTorch NT123A flashlight batteries. Consumers should stop using recalled products immediately unless otherwise instructed. It is illegal to resell or attempt to resell a recalled consumer product. The batteries can overheat and rupture, posing a fire and burn hazard to consumers. There has been one report of NexTorch NT123A flashlight batteries rupturing and catching fire, causing burns to the consumer's body, clothes, and vehicle. The recalled product is a NexTorch NT123A flashlight battery, bearing the trademark superscript, rather than registered trademark superscript. Its body is silver metallic-colored and has the NexTorch logo and the voltage (3 V) on it. The battery is often packaged with NexTorch flashlights. The batteries were sold at firearm dealers and law enforcement supply stores, and on the Web, including Amazon.com and the firm's Web site www.nextorch.com, from July 2007 to July 2011. Consumers should immediately stop use of the battery and contact NexTorch for instructions on how to receive a free replacement. Source: <http://www.cpsc.gov/cpscpub/prerel/prhtml11/11296.html>

NHTSA recall notice - Chrysler Town and Country, Voyager, Dodge Grand Caravan mini-vans. Chrysler is recalling 299,718 Chrysler Grand Voyager, Town and Country, and Dodge Grand

UNCLASSIFIED

UNCLASSIFIED

Caravan vehicles manufactured from June 24, 2007, through July 30, 2008 (model year 2008 vehicles.) These vehicles may experience a heating and air conditioner (HVAC) condensate leak from the HVAC drain grommet onto the occupant restraint control module that can lead to the illumination of the airbag warning light, and a potential inadvertent airbag deployment without warning. An inadvertent airbag deployment could result in injury to the seat occupant in front of the deploying airbag and/or a vehicle crash. Dealers will replace the affected air bag module free of charge. The safety recall is expected to begin during August 2011. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V39400&summary=true&prod_id=927772&PrintVersion=YES

Nissan recalling 20,000 new Altimas. Nissan Motor Co. said July 31 it is recalling about 20,000 2011 and 2012 Altima sedans over concerns a front suspension bolt might not have been properly tightened. In a notice posted on the National Highway Traffic Safety Administration Web site, Nissan said some vehicles might have transverse link bolts that weren't properly tightened. This could allow the bolt to become loose and cause a rattling noise or vibration. Nissan said in the unlikely event a bolt comes out completely, a driver could experience difficulty controlling the vehicle. The recalled vehicles were assembled at Nissan's Canton, Mississippi assembly plant. Nissan notified dealers of the planned recall July 18, and started notifying owners August 1. Dealers are checking the bolts on new vehicles before selling them. Source:

<http://www.detnews.com/article/20110731/AUTO01/107310318/1148/auto01/Nissan-recalling-20-000-new-Altimas>

NHTSA recall notice - Ford F-150, F-250, and Lincoln Blackwood trucks. Ford is recalling 1.1 million 1997 through 2003 model year Ford F-150, 2004 model year Ford F-150 Heritage, 1997 through 1999 model year F-250 less than 8,500 pounds gross weight rating, and 2002 and 2003 Lincoln Blackwood vehicles manufactured from June 20, 1995 through August 4, 2004 originally sold, or currently registered in, Connecticut, Delaware, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, New Hampshire, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, Vermont, West Virginia, Wisconsin, and the District of Columbia. Prolonged exposure to road deicing chemicals may cause severe corrosion of the fuel tank straps that secure the tank to the vehicle. As a result of the corrosion, one or both straps may fail allowing the fuel lines to separate from the tank, or in some cases, causing the tank to contact the ground. Either scenario may result in a fuel leak presenting a fire hazard. Ford will notify owners and instruct them to take their vehicles to a Ford or Lincoln dealer to have the fuel tank straps replaced with straps that have increased corrosion protection. Early in this campaign, if replacement straps are not available, dealers may install a cable support under the strap as an interim repair, or a steel reinforcement over existing strap as a permanent repair. Any repairs will be performed free of charge. The safety recall is expected to begin on or about September 12. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V38500&summary=true&prod_id=215099&PrintVersion=YES

UNCLASSIFIED

DEFENSE/ INDUSTRY BASE SECTOR

F-35s grounded after electrical system fault. F-35 Lightning II program officials have grounded all jets while they investigate an electrical fault aboard one of the U.S. Air Force A-model birds, according to an announcement August 3. The grounding — the program's third in the past year — was ordered after a power failure August 2 aboard the Air Force jet as it was running its engine while still on the ground, not during flight. No injuries to the pilot or ground crew occurred. The F-35's IPP is a turbo-machine that provides power to start the engine and generates cooling for the aircraft. The government and contractor engineering teams are reviewing data from the incident to determine the root cause of the failure. Officials implemented a precautionary suspension of operations until the F-35 engineering, technical, and system safety teams fully understand the cause of the incident. Once the facts are understood, a determination will be made when to lift the suspension and begin ground and flight operations of the 20 F-35s currently in flying status. These aircraft are part of the System Development and Demonstration (SDD) and Low Rate Initial Production (LRIP) fleet. Source: <http://www.dodbuzz.com/2011/08/03/f-35s-grounded-after-electrical-system-fault/>

Anonymous hacks U.S. gov contractor, airs dirty laundry. Members of the Anonymous hacking collective said they broke into the networks of Mantech International and stole internal documents belonging to the U.S. government contractor, The Register reported July 30. As proof, the members posted a 390 MB download that appeared to contain reports related to the North Atlantic Treaty Organization, the U.S. Army, and personnel files. A note that accompanied the Bittorrent file said the hack was intended to defy the FBI, which last week charged 14 people of participating in an Anonymous-led Web attack in December that created service disruptions for some PayPal customers. The leaked documents appeared to have little or no connection to the FBI, although press releases appeared to show the FBI has outsourced some of its IT security to Mantech. The Washington, D.C.-based firm has also signed contracts to provide services to the departments of Defense, State, Homeland Security, Energy, and Justice. Mantech neither confirmed nor denied the Anonymous claims Mantech was compromised "utterly and thoroughly" [sic]. Source: http://www.theregister.co.uk/2011/07/30/anonymous_claims_mantech_hack/

EMERGENCY SERVICES

Hackers could spring killers from prison. At the DefCon hacker conference in Las Vegas, Nevada, a security consultant demonstrated how a hacker could take advantage of a prison's programmable logic controller (PLC) — small computers used for machine automation — to remotely control the locks on prison cells, Wired reported. PLCs are the same technologies exploited by the infamous Stuxnet worm, which targeted power plants in Iran. The consultant has engineered or consulted on electronic security systems in more than 100 prisons, courthouses, and police stations in the United States. He and his team presented their findings to the FBI and other federal agencies. Although they will not disclose the vulnerabilities they preyed on at the DefCon conference, the consultant said the flaws they cracked could grant a hacker control of a prison. Although it would take some work to infiltrate the prison's security

UNCLASSIFIED

system — a hacker would have to put malware on the network through an infected USB drive or a spear-phishing attack aimed at a prison employee — the possibilities appear endless.

Source: http://www.msnbc.msn.com/id/43975446/ns/technology_and_science-security/#.TjJJaWGzpbA

(Colorado) Cyanide scare sign of growing 'chemical suicide' problem. Six people were recovering August 2 after they walked into an apartment in Colorado Springs, Colorado, that was filled with a deadly chemical. Firefighters were called to an apartment off of Chestnut Street August 1 for a welfare check. When they walked inside, they found a body surrounded by a powder and an open bottle labeled "Sodium Cyanide." As a precautionary measure, three paramedics, one police officer, and two other people were taken to the hospital to be treated for exposure. Experts sidy this is a growing trend called "chemical suicide" or "detergent suicide." The captain of the hazmat team of the Denver Fire Department and his hazMat team are training the Denver Fire Department for dealing with this trend. Source:

<http://www.9news.com/news/article/211452/188/Cyanide-scare-sign-of-growing-chemical-suicide-problem>

(Delaware) Chemical fumes coming from vehicle at service plaza sicken 2 troopers. Delaware State Police are currently investigating an incident that left two troopers ill from apparent exposure from a chemical coming from a car trunk at the Newark Sevice Plaza in Newark, Delaware. An early report indicated the troopers were overcome by fumes from the trunk of an abandoned vehicle parked by the fuel pumps at the Sunoco in the I-95 Service Plaza, south of Newark at about 7:05 a.m. The troopers were transported to the Christiana Hospital where they were being treated for non-life-threatening exposure to an unknown chemical. A perimeter was set up around the vehicle until a hazardous materials team from the department of natural resources and environmental control and the responding fire companies could respond. The vehicle has since been declared safe. This incident is still being investigated.

Source:

<http://www.newarkpostonline.com/articles/2011/08/02/news/doc4e380d780f712315286912.txt>

Hackers dump secret info for thousands of cops. Hackers said they posted the names, addresses, and other personal information of 7,000 law enforcement officers that were stolen from a Missouri Sheriff's Association training academy Web site they compromised, The Register reported August 1. One of the identified individuals confirmed with The Register that the data listed for him in the 938 kilobyte file was accurate. Many of the entries include officers' Social Security numbers, e-mail addresses, and the usernames and passwords for their accounts on the Web site. AntiSec claimed responsibility and said the data dump was made in retaliation for the recent arrest of 14 people accused of participating in a Web attack in December that strained server capacity for PayPal. Many of the passwords employed by the officers were ordinary dictionary words, or were identical to their names or badge numbers, demonstrating some of the same mistakes other users make in setting up security pass codes. Assuming the officers used the same password for other accounts, as is common, their e-mail accounts would also be compromised. The file suggests the training site failed to follow industry best practices

UNCLASSIFIED

UNCLASSIFIED

by securing the password database with one-time hashes to prevent them from being read by attackers. Source: http://www.theregister.co.uk/2011/08/01/missouri_cops_hacked/

ENERGY

(North Carolina) Oil spill caused by theft at electrical substation. A theft at an electrical substation in Surry County, North Carolina, caused a 1,420-gallon oil spill the weekend of July 30 and 31, investigators said. The Surry County Sheriff's Office responded to the crime, reported July 30 at a Surry-Yadkin Electric Membership facility at 558 Ararat-Longhill Road in Pilot Mountain. A sheriff said August 1 the incident targeted copper wiring contained within five electrical-distribution transformers at the site that were accessed after a section of a fence was cut. The transformers contained mineral oil, and after their steel covers were removed, the oil was drained to facilitate the wire theft. Electrical transformers are filled with mineral oil to achieve desired electrical and chemical properties. Those targeted in the weekend incident weighed about 300 pounds each. The sheriff said he was not aware of disruptions in service to electrical customers of the area surrounding the theft, speculating that backup transformers might have been involved rather than ones that were online. Members of Bannertown Volunteer Fire Department responded to the spill, which required a clean-up. Surry-Yadkin Electric had a private environmental company respond. Source: http://www.mtairynews.com/view/full_story/14916564/article-Oil-spill-caused-by-theft-at-electrical-substation?instance=secondary_news_left_column

FOOD AND AGRICULTURE

USDA scientists study effects of rising carbon dioxide on rangelands. Rising carbon dioxide (CO₂) levels can reverse the drying effects of predicted higher temperatures on semi-arid rangelands, according to a study published today in the scientific journal *Nature* by a team of U.S. Department of Agriculture (USDA) and university scientists. Warmer temperatures increase water loss to the atmosphere, leading to drier soils. In contrast, higher CO₂ levels cause leaf stomatal pores to partly close, lessening the amount of water vapor that escapes and the amount of water plants draw from soil. This study finds CO₂ does more to counterbalance warming-induced water loss than previously expected. In fact, simulations of levels of warming and CO₂ predicted for later this century demonstrated no net change in soil water, and actually increased levels of plant growth for warm-season grasses. The results cover the first 4 years of the 8-year Prairie Heating and CO₂ Enrichment (PHACE) experiment on native northern mixed grass rangeland. The study is being conducted by the USDA's Agricultural Research Service (ARS) Rangeland Resources Research Unit (RRRU) at the High Plains Grasslands Research Station near Cheyenne, Wyoming. An ARS plant physiologist led the study, which uses both CO₂ pipelines and thermal infrared heaters to simulate global warming conditions predicted for the end of the century: 600 parts per million (ppm) of CO₂ — compared to today's average 390 ppm — and day/night temperatures raised by 3 and 5 degrees Fahrenheit, respectively. Source: <http://www.ars.usda.gov/is/pr/2011/110803.htm>

UNCLASSIFIED

UNCLASSIFIED

Arkansas) Cargill recalls 36 million pounds of ground turkey. Cargill announced August 3 it is recalling almost 36 million pounds of ground turkey products that may be contaminated with a multi-drug resistant strain of Salmonella Heidelberg, a pathogen linked to at least 76 illnesses across the United States, and one death in California. The recalled meat came from a single processing facility in Springdale, Arkansas, but ended up in dozens of different ground turkey products sold nationwide under a variety of brand names including Honeysuckle White, Shady Brook Farms, Riverside, Aldi's Fit and Active Fresh, Spartan, Giant Eagle, Kroger, and Safeway. Cargill is recalling products produced between February 20 through August 2, and halting production of ground turkey products at the facility until the source of contamination is identified and corrected. The Centers for Disease Control and Prevention (CDC) announced the agency found four retail ground turkey samples to be positive for the same strain of Salmonella Heidelberg between early March and late June. The samples were taken as part of routine sampling for the National Antimicrobial Resistance Monitoring System, and had "not been linked to illnesses" so they did not spark a recall. As late as August 2, U.S. Department of Agriculture Food Safety and Inspection Service officials said there was not enough evidence to substantiate a recall. The agency said August 3 that epidemiologic and traceback investigations, as well as in-plant findings, led the agency to determine there is a link between the Cargill ground turkey products and the outbreak. Source:

<http://www.foodsafetynews.com/2011/08/cargill-recalls-36-million-pounds-of-ground-turkey/>

Government seeking source of tainted turkey. The U.S. Department of Agriculture (USDA) and the U.S. Centers for Disease Control and Prevention (CDC) are looking for the source of a salmonella outbreak, dating back to March, which has resulted in 76 illnesses and 1 death. California state health officials said August 2 the one death was in Sacramento County. Seventy-six people in 26 states have been made sick from the same strain of the disease. The CDC said August 1 that cultures of ground turkey from four retail locations between March 7 and June 27 showed contamination with the same strain of salmonella, though those samples were not specifically linked to the illnesses. The agency said preliminary data showed three samples were linked to the same production establishment, but it did not name the retailers or manufacturers. The lack of information may be attributed to USDA rules that make it harder to investigate and recall salmonella-tainted poultry. Officials must directly link the illnesses with a certain producer or establishment, which is difficult to do because people do not always remember what they ate or where they bought it. It appears officials have not been able to prove the link between the samples of salmonella they found — even though they are the same strain — and the 77 people who were sickened. The states with the highest number sickened were Michigan and Ohio, 10 illnesses each, while nine illnesses were reported in Texas. Illinois had seven, California six, and Pennsylvania five. Source:

<http://kstp.com/news/stories/S2225705.shtml?cat=1>

(Hawaii) New pest killing bee hives in Hawaii. Experts from the University of Hawaii and the state agriculture department have begun meeting with beekeepers across Hawaii to teach them how to protect their hives against a new beetle pest that can ruin their honey production. The beetles can contaminate honey and cause bees to abandon their hives. Small hive beetles are 4 or 5 millimeters long, but they can have a big negative effect on agriculture. They have

UNCLASSIFIED

UNCLASSIFIED

turned up in beehives on Oahu, the Big Island and more recently, Maui and Molokai. "Beekeepers are losing colonies, so we're trying to help them rebuild," said an apiculture specialist with the state department of agriculture. Agriculture officials said bees pollinate food crops of all sorts, from macadamia nuts, cucumbers, watermelons, and avocados to coffee, mangoes, and lychee. The small hive beetles came from Africa and arrived in the United States around 1996. Since then, they have spread throughout the country. Another pest, called the varroa mite, has already devastated some honey operations across Hawaii as well. Source: <http://www.kitv.com/news/28748668/detail.html>

(Georgia; Florida; Alabama) Company expands food recall. Flying Food Group, a Lawrenceville, Georgia-based company that provides food for Starbucks and RaceTrac, has recalled 40 types of sandwiches, wraps, parfaits, and other items, temporarily shutting down its operations due to a possible listeria contamination. No illnesses have been reported to date, but the U.S. Food and Drug Administration has requested that products recently manufactured at the Lawrenceville facility be recalled. The potential for a contamination by listeria monocytogenes was discovered after sampling and testing conducted by the Georgia Department of Agriculture revealed the bacteria's presence in one of the products, officials said. The recent recall — an expansion of one initiated July 19 by the U.S. Department of Agriculture — includes products made for Core-mark Atlanta Division, RaceTrac, and Starbucks. Core-mark products were distributed to outlets in Alabama, Georgia, and Florida. Starbucks products were distributed in Alabama and Georgia, while RaceTrac products were distributed only in Georgia. Source: http://www.gwinnettdailypost.com/localnews/headlines/Company_expands_food_recall_126560888.html

Homeland Security to regulate fertilizer chemical used in Oklahoma City, Norway Bombings. More than 15 years after a fertilizer bomb was used to blow up a government building in Oklahoma City, killing 168 people, the federal government is proposing to regulate the sale and transfer of the chemical ammonium nitrate. The proposal comes nearly 4 years after Congress gave the DHS the authority to develop a program to regulate the compound. Ammonium nitrate is one of the most common farm fertilizers in the world, and instructions for turning it into a bomb are available on the Internet. Its deadly potential was once again realized July 22, when a Norwegian man allegedly blew up a government building in Norway, killing eight people with a bomb that investigators believe was made with ammonium nitrate. On August 2, the DHS proposal is expected to be posted on the Federal Register Web site and the public will have 120 days to comment. As it's proposed, the "Ammonium Nitrate Security Program" would require those who purchase, sell or transfer at least 25 pounds of the chemical in the United States to register with the government so they may be screened against U.S. terror watch lists, according to a homeland security official who spoke on condition of anonymity because the proposal had not formally been published. The DHS would give registration numbers to those who are approved to buy, sell or transfer ammonium nitrate. The registrants would also be required to keep records and report the theft or loss of the chemical within 24 hours of discovering it missing. A number of countries have banned ammonium nitrate fertilizer. And some U.S. states regulated its use after the chemical was used in the Oklahoma City bombing. Last year, the Afghan government banned ammonium nitrate, as the chemical most often used

UNCLASSIFIED

UNCLASSIFIED

in bombs targeting American soldiers in Afghanistan. Source:

<http://www.foxnews.com/politics/2011/08/02/homeland-security-to-regulate-fertilizer-chemical-used-in-oklahoma-city-norway/>

National health alert issued for ground turkey. An outbreak already infecting 77 people in 26 states with Salmonella Heidelberg prompted an unusual public health alert late July 29 about the "critical importance" of safe handling of ground turkey. The alert about all frozen and fresh ground turkey was issued by the U.S. Department of Agriculture (USDA) through its Food Safety and Inspection Service (FSIS). A public health alert not involving a specific brand or product recall is a rare action for the USDA. With the public health alert came the first notice that the federal Centers for Disease Control and Prevention (CDC), and state health departments have identified and are investigating the multistate outbreak of Salmonella Heidelberg. "The public health alert was initiated after continuous medical reports, ongoing investigations and testing conducted by various departments of health across the nation determined there is an association between consumption of ground turkey products and an estimated 77 illnesses reported in 26 states," the USDA statement said. The CDC and state health departments made the link through epidemiological investigation and pulsed-field gel electrophoresis analysis, the FSIS said. While the CDC and state health departments are investigating, the FSIS noted it is working to determine the source of the contamination. Source:

<http://www.foodsafetynews.com/2011/07/national-health-alert-issued-for-ground-turkey/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(New York) Bomb scare causes evacuation at IRS building. The Internal Revenue Service (IRS) building in Riverhead, New York, was evacuated August 3 after police received a report of a "suspicious package" in the rear of the building, Riverhead Police said in a statement. The package, a suitcase found underneath an air conditioner in the rear of the IRS building, was reported to police by a security official at 8:30 a.m. The building was evacuated as a precaution. The Suffolk County Police Bomb Unit responded to the strange package and sent a robot to investigate. An X-ray of the case revealed an unknown electronic device inside, but upon opening the suitcase, police discovered it was filled with clothing and other "harmless items." The case was dubbed a false alarm, and those evacuated were allowed back into the building. Source: <http://riverhead.patch.com/articles/bomb-scare-causes-evacuation-at-irs-building>

(Missouri) Suspicious substance being investigated at IRS building in KC. Firefighters in Kansas City, Missouri, were called to the Internal Revenue Service building near Union Station to check on an unknown substance reportedly found in the mail August 2. Dispatchers sent crews about 2:10 p.m. to the building at 333 W. Pershing Road. Fire officials said about 90 people were in the area where the substance was found, and they were being kept together away from other people as a precaution while firefighters determine what the substance is. No one showed any signs or symptoms of exposure to a hazardous material, according to fire officials. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.kansascity.com/2011/08/02/3052507/suspicious-substance-being-investigated.html>

(District of Columbia) Intruder climbs White House fence. A 41-year-old homeless man climbed the White House fence in Washington D.C. about 7:45 p.m. August 2. The man made it onto the north side of the White House grounds, but he was quickly taken into custody by the U.S. Secret Service, authorities said. He was taken to a D.C. police station for processing, a Secret Service spokesman said. He said the man would be charged with unlawful entry and contempt of court. The contempt charge was to be brought in connection with an order requiring the man to stay away from the White House. It was not clear why he climbed the fence, and authorities did not think that he was armed. A backpack that apparently belonged to him was being examined. The last event on the U.S. President's official schedule was set for 4:30 p.m. In an unusual twist, a 6-year-old girl reached the lawn July 31 by going through the fence. After slipping between the black metal pickets, she was escorted out to her parents by the Secret Service, authorities said. Source: http://www.washingtonpost.com/local/intruder-climbs-white-house-fence/2011/08/02/gIQAxmVmql_story.html?hpid=z4

State actor seen behind enormous wave of cyber attacks. Security company McAfee discovered the biggest series of cyber attacks to date, involving the infiltration of the networks of 72 organizations including the United Nations, governments, and companies around the world, Reuters reported August 3. McAfee said it believed there was one "state actor" behind the attacks but declined to name it, though one security expert briefed on the hacking said the evidence points to China. The long list of victims in the 5-year campaign include the governments of the United States, Taiwan, India, South Korea, Vietnam and Canada; the Association of Southeast Asian Nations; the International Olympic Committee; the World Anti-Doping Agency; and an array of companies, from defense contractors to high-tech enterprises. In the case of the United Nations, the hackers broke into the computer system of its secretariat in Geneva in 2008, hid there for nearly 2 years, and quietly combed through reams of secret data. McAfee learned of the extent of the hacking campaign in March of this year when its researchers discovered logs of the attacks while reviewing the contents of a "command and control" server they discovered in 2009 as part of an investigation into security breaches at defense companies. It dubbed the attacks "Operation Shady RAT" and said the earliest breaches date back to mid-2006, though there might have been other intrusions. (RAT stands for "remote access tool," a type of software hackers and security experts use to access computer networks from afar). McAfee's vice president of threat research said McAfee had notified all 72 victims of the attacks, which are under investigation by law enforcement agencies around the world. Source: <http://www.reuters.com/article/2011/08/03/us-cyberattacks-idUSTRE7720HU20110803>

(Oregon) Letter with white substance sent to congressman's office. An envelope containing a 3-page type-written letter and a suspicious white substance was found August 1 at a U.S. Congressman's office on State Street in Salem, Oregon. The letter came a day after the U.S. President and congressional leaders reached a tentative deal to increase the nation's debt ceiling, and 3 days after the Congressman circulated a letter opposing the GOP's plan to cut

UNCLASSIFIED

UNCLASSIFIED

spending. Though the Congressman was not in the office at the time, three of his employees were there and at least one called authorities about possible hazardous materials in the envelope. FBI agents responded and took the envelope to be tested. Oregon State Police, Salem Fire Hazmat Team 13, Salem Police, and Salem Public Works responded to a report of possible hazardous materials at the office at around 8:30 a.m. The building was evacuated. Salem Police closed three of State Street's four lanes for about 90 minutes. Workers in the Congressman's office and employees who work in other offices in the facility were allowed to return to the building soon after. Source:

<http://community.statesmanjournal.com/blogs/crimeandcourts/2011/08/01/letter-with-white-powder-sent-to-congressmans-office>

Anonymous threat at U.S. Consulate considered false. An anonymous threat called in from a public telephone in Tijuana, Mexico, July 29 brought law enforcement agencies to the newly opened offices of the U.S. Consulate General in the city's Mesa de Otay section, authorities said. A spokesman for Mexico's Baja California Public Security Secretariat said the state's communications center received a call shortly before 10:30 a.m. reporting that "armed persons were going attack the American Consulate." He said the call turned out to be a false alarm. A U.S. Consulate official acknowledged the anonymous call, but said the facilities remained open. Source: <http://www.signonsandiego.com/news/2011/jul/29/anonymous-threat-us-consulate-considered-false/>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Anonymous unsheathes new, potent attack weapon. Members of Anonymous are developing a new attack tool as an alternative to the LOIC (Low Orbit Ion Cannon) DDoS utility. The move follows a spate of arrests thought to be connected to use of the LOIC, which by default does nothing to hide a user's identity. The new tool, dubbed RefRef, due to be released in September, uses a different approach to knocking out Web sites. LOIC floods a targeted site with TCP or UDP packets, a relatively unsophisticated yet effective approach, especially when thousands of users use the tool to join voluntary botnets. RefRef, by contrast, is based on a more sophisticated application-level approach designed to tie up or crash the servers behind targeted Web sites instead of simply flooding them with junk traffic, according to a blog post on the development by an Anonymous-affiliated blog. Arrests in England, Spain, and Turkey connected to LOIC-powered attacks have already prompted some core members of Anonymous to move towards using a new server and dropping LOIC in favor of other attack tools, such as Slow Loris and Keep-Dead DoS. This now seems to be purely a stop-gap measure while RefRef is under development. Source:

http://www.theregister.co.uk/2011/08/04/anon_develops_loic_ddos_alternative/

Researcher follows RSA hacking trail to China. Malware used in the attack against RSA Security earlier this year was controlled from China, a well-known botnet researcher said August 3. The director of malware research for Dell SecureWorks, traced the command-and-control (C&C) servers used to oversee the RSA attack to networks in Beijing and Shanghai. "This gives us the where, but not the who," he said when asked whether his work had come up with clues about

UNCLASSIFIED

UNCLASSIFIED

the attack's architects. In mid-March, RSA confirmed it had been targeted by hackers who had breached its network defenses and stole proprietary information. Although RSA never detailed what was stolen, it admitted data related to the company's SecurID two-factor authentication products was part of the haul. The attack was expensive for RSA, which in a recent earnings report said it had spent \$66 million to replace customers' SecurID tokens that are used by many defense contractors and government agencies. The attackers gained access to RSA's network by convincing a small number of the company's employees to open malware-infected Excel spreadsheets. The spreadsheets included an exploit for a then-unpatched vulnerability in Adobe's Flash Player. Later attacks on defense contractor Lockheed Martin reportedly utilized information obtained in the RSA hack. In his months-long project, the researcher uncovered the location of the malware's command servers by using error messages displayed by a popular tool called "HTran", which Chinese hackers often bundle with their code. HTran bounces traffic between multiple IP addresses to mask the real identity of the order-giving servers, making it appear, for instance, that the C&C servers are in the United States when they are not. Source: http://www.computerworld.com/s/article/9218857/Researcher_follows_RSA_hacking_trail_to_China

A unique malware file is created every half-second. Sophos has released its Mid-Year 2011 Security Threat Report, which reveals that since the beginning of 2011, the company has identified an average of 150,000 malware samples every day. This equates to a unique malware file being created every half-second, a 60 percent increase since 2010. In addition, around 19,000 malicious Web site addresses (URLs) are now identified daily, with 80 percent of those URLs being pages on legitimate Web sites that have been hacked or compromised. High-profile hacking attacks against governments and corporations have dominated the security landscape in 2011. The result is that other security issues that could pose a greater threat to businesses, governments, and consumers have received less attention. Source: <http://www.net-security.org/secworld.php?id=11371>

Researchers warn of SCADA equipment discoverable via Google. A demonstration August 2 during a Black Hat conference workshop revealed that Supervisory Control and Data Acquisition (SCADA) systems used to run power plants and other critical infrastructure lack many security precautions to keep hackers out, and that operators sometimes advertise their wares on Google search. The chief technology officer at security consultancy FusionX typed in search terms associated with a Programmable Logic Controller (PLC), an embedded computer used for automating functions of electromechanical processes. Among the results was one referencing a "RTU pump status" for a Remote Terminal Unit, such as those used in water treatment plants and pipelines, that appeared to be connected to the Internet. The result also included a password — "1234". Most SCADA protocols do not use encryption or authentication, and they do not have access control built into them or the device itself, said a fellow presenter and founder of Red Tiger Security. This means that when a PLC has a Web server and is connected to the Internet, anyone who can discover the Internet Protocol address can send commands to the device and the commands will be performed. "If that RTU or PLC has large motors connected to it, pumping out water or chemicals, the equipment could be turned off," the Red Tiger Security founder said. "If it was a substation and the power recloser switches were closed,

UNCLASSIFIED

UNCLASSIFIED

we could break it open and create an (electricity) outage for an entire area or city ... The bottom line is you could cause physical damage to whatever is connected to that PLC." Source: http://news.cnet.com/8301-27080_3-20087201-245/researchers-warn-of-scada-equipment-discoverable-via-google/?part=rss&tag=feed&subj=InSecurityComplex

Spear-phishing and crimeware assembling marked second half of 2010. The Anti-Phishing Working Group (APWG) reports the development of crimeware surged in the half-year period ending in December 2010, with one data contributor registering more than 10 million new malware samples in the period, while other analysts describe important shifts in approaches to crimeware deployment by cybercrime gangs. Cybercriminals repurpose base code of existing crimeware using polymorphic techniques to craft new variations of crimeware to evade detection by filters reliant on fingerprints of known crimeware. A PandaLabs technical director said 55 percent of the new samples created in the 2nd half of 2010 were Trojans, the favorite weapon used by cybercriminals to infect consumers' computers. A senior manager at Security Research for Websense said his laboratory noticed a shift toward a binary weapons approach to infecting PCs with crimeware, assembling the final crimeware code from several components that arrive through different mechanisms, and at different times. While measurements for conventional social engineering-based phishing showed some slowing of growth in the 2nd half of 2010, reports of hyper-focused phishing attacks on key personnel have been increasing since then, and have continued growing through early 2011, indicating a larger shift in tactics by established cybercrime gangs. Source: <http://www.net-security.org/secworld.php?id=11373>

Anonymous develops new denial of service tool. Anonymous supporters appear to have built a new denial of service tool that is said to exploit SQL vulnerabilities to support the group's future campaigns. The tool is very effective, a 17-second attack from a single machine resulted in a 42-minute outage on Pastebin July 29, Softpedia reported July 30. According to The Tech Herald which spoke with its creators, the new tool is called RefRef and is developed in JavaScript. This means that it works in any modern browser on any operating system, including those in smartphones and tablets. The effectiveness of RefRef is due to the fact it exploits a vulnerability in a widespread SQL service. The tool works by turning the servers against themselves. It sends malformed SQL queries carrying the payload, which in turn forces the servers to exhaust their own resources. The flaw is apparently known but not widely patched yet. The tool's creators do not expect their attacks to work on a high-profile target more than a couple of times before being blocked, but they do not believe organizations will rush to patch this flaw en masse before being hit. Source: <http://news.softpedia.com/news/Anonymous-Develops-New-Denial-of-Service-Tool-214313.shtml>

Millions hit in South Korean hack. South Korea has blamed Chinese hackers for stealing data from 35 million accounts on a popular social network. The attacks were directed at the Cyworld Web site as well as the Nate Web portal, both run by SK Communications. Hackers are believed to have stolen phone numbers, e-mail addresses, names, and encrypted information about the sites' many millions of members. It follows a series of recent cyber attacks directed at South Korea's government and financial firms. Government ministries, the National Assembly, the country's military HQ, and networks of U.S. Forces based in Korea were also hit. The Korean

UNCLASSIFIED

UNCLASSIFIED

Communications Commission claimed to have traced the source of the incursion back to computer IP addresses based in China. Source: <http://www.bbc.co.uk/news/technology-14323787>

Sneaky trojan exploits e-commerce flaws. A security flaw in osCommerce, an open source e-commerce package, created a means for criminals to compromise 90,000 Web pages with redirection scripts that ultimately directed surfers towards a site serving up an exploit toolkit designed to compromise visitors' PCs. "The attackers inserted an iframe that leads to certain URLs in each of these sites, triggering several redirections," an analysis of the attack published by Trend Micro explains. "The redirections finally lead to an exploit kit that abuses the following vulnerabilities in an attempt to download a malicious file onto systems," it noted. "This malware searches for internet caches, cookies, and histories in order to steal login credentials and other data used for specific websites, usually banks and other financial institutions," Trend Micro adds. "Joric-BRU then forwards the stolen information to specific websites." The attack plants exploit code on e-commerce sites, where surfers expect a more trusted environment. In addition, the malware used in the attack attempts to delete itself from compromised systems after riffling compromised systems for log-in credentials, a feature that differentiates the banking trojan from better known threats such as the Zeus Trojan. Older versions of osCommerce are subject to a directory traversal vulnerability as well as an XSS vulnerability for version 2.2-MS2. Source:

http://www.theregister.co.uk/2011/08/01/banking_trojan_exploits_ecommerce_website_flaws/

SecurID data breach cost RSA \$66 million. A data breach that resulted in the theft of information related to its SecurID authentication product cost RSA Security and its parent company EMC \$66 million so far. According to the Washington Post, the sum was revealed in an earnings call July 26. The costs included expenses associated with monitoring the networks of defense contractors, federal agencies, and other customers who expressed concerns over the integrity of the product after the breach. The intrusion occurred in March and was the result of a spear phishing attack against RSA employees that exploited a zero-day Flash Player vulnerability. The company was very vague following the breach saying only that information regarding its SecurID product was targeted, but that its customers were not at risk. RSA was criticized by the information security community for its lack of transparency regarding this incident, and in May it was reported that a cyber attack against Lockheed Martin involved cloned SecurID devices. Following the attack and the revelation that other military contractors might also have been targeted as a result of its data breach, RSA Security offered to replace all SecurID tokens for concerned customers. Source: <http://news.softpedia.com/news/SecurID-Data-Breach-Costs-RSA-66-Million-214318.shtml>

NATIONAL MONUMENTS AND ICONS

(California) **Mendocino forest pot sweep up to 545,000 plants.** A major multi-county, multi-agency crackdown on marijuana growing in the Mendocino National Forest in California as of August 3 had yielded 545,313 pot plants, 120 arrests, and 36 weapons, officials said. The

UNCLASSIFIED

UNCLASSIFIED

number of plants seized since Operation Full Court Press began July 18 has now surpassed the 465,000 plants seized in 2010 during a similar operation called Operation Trident in the Central Valley. Operation Trident encompassed three counties, but had about the same force of 300 to 400 people. Twenty-five local, state, and federal agencies are taking part in this year's 3-week eradication and cleanup efforts. Operation Full Court Press is taking place in the six Northern California counties that have portions of the Mendocino National Forest: Mendocino, Lake, Colusa, Trinity, Tehama, and Glenn. The operation stems from complaints the national forests have been taken over by armed marijuana growers who have made public lands unsafe for citizens, and who wreak environmental damage and leave behind toxic chemicals and garbage. Nearly 50,000 pounds of trash and 86 pounds of pesticides have been removed from the forest during the operation, and cleanup will continue after the eradication operation ends. Source: <http://www.pressdemocrat.com/article/20110803/ARTICLES/110809811/1350?Title=Mendocino-forest-pot-sweep-up-to-545-000-plants>

(Massachusetts) Massive blaze guts historic inn. Fire officials in Groton, Massachusetts were investigating what caused a massive, four-alarm fire that gutted a historic, 300-year-old inn August 2. Fire crews said the fire broke out about 9:30 p.m. at the historic Old Groton Inn on Main Street. Crews from 15 neighboring communities were called in to help battle the fire. Officials said the inn was also known as the Stagecoach Inn and dated back to 1678. It was put on the National Register of Historic Places in 1976. According to the Web site, it was one of the region's oldest dining and lodging establishments. Town residents were asked to conserve water August 3 because so much was used fighting the fire. Source: <http://www.thebostonchannel.com/news/28747450/detail.html>

(California) Historic fire lookout burns east of Springville. The Needles Fire Lookout Tower was destroyed July 28 in a structure fire unrelated to the Lion Wildland Fire in the Golden Trout Wilderness of Sequoia National Forest and parts of Sequoia National Park in California. The tower was located east of the Ponderosa Lodge on the Western Divide Highway. The loss of the tower severed a vital communication line for the 160 firefighters battling the the almost 17,500-acre Lion Wildland Fire, a district ranger said. The U.S. Forest Service employee operating the tower got out safely, she said. The lookout was also used as the employee's office and home during fire season in the summer months. Built in 1937-1938 by the Civilian Conservation Corps on top of a rock formation, the lookout tower at 8,245 feet allowed staff to detect fires as far away as Mt. Whitney, including the Kern River drainage, Olancho Peak, Farewell Gap, and Dome Rock. Source: <http://www.visaliatimesdelta.com/article/20110729/NEWS01/110729005>

POSTAL AND SHIPPING

Nothing Significant to Report

UNCLASSIFIED

UNCLASSIFIED

PUBLIC HEALTH

Insulin pumps, monitors vulnerable to hacking. A security researcher who is diabetic has identified flaws that could allow an attacker to remotely control insulin pumps and alter the readouts of blood-sugar monitors. As a result, diabetics could get too much or too little insulin, a hormone they need for proper metabolism. The researcher, a diabetic who experimented on his own equipment, shared his findings with the Associated Press before releasing them August 4 at the Black Hat computer security conference in Las Vegas, Nevada. Although there is no evidence anyone has used his techniques, his findings raise fears about the safety of medical devices as they are brought into the Internet age. Serious attacks have already been demonstrated against pacemakers and defibrillators. Though there has been a push to automate medical devices and include wireless chips, the devices are typically too small to house processors powerful enough to perform advanced encryption to scramble their communications. As a result, most devices are vulnerable. Source:

<http://news.yahoo.com/insulin-pumps-monitors-vulnerable-hacking-100605899.html>

FDA warns of counterfeit 'morning-after' pill. The U.S. Food and Drug Administration (FDA) said the emergency "morning after" birth control pill Evital could be counterfeit and may not be safe or prevent pregnancy. The agency is asking women not to use the medication. Evital is not approved for use in the United States. But the FDA said, while it does not have evidence of "pattern targeting" of a specific ethnic group, the drug may have been distributed in Hispanic communities under the label "Evital Anticonceptivo de emergencia, 1.5mg, 1 tablet by Fluter Domull." The FDA is asking consumers to contact their doctor if they have taken the pills and had any side effects. It also is asking anyone with information about the pills to contact their Center for Drug Evaluation and Research/Ingredient Adulteration. Any information gathered will be used to get Evital off the market. Source:

http://thechart.blogs.cnn.com/2011/08/01/fda-warns-of-counterfeit-morning-after-pill/?hpt=he_c2

(Idaho) ISU breach exposes medical information. A breach in an Idaho State University server's firewall has exposed private medical information from patients of Pocatello Family Medicine in Pocatello to anyone on the Internet, KIFI 8 Idaho Falls reported August 1. The clinic said there is no evidence any of that medical information has been stolen or even accessed. They say the firewall was taken down in August 2010 for maintenance, but an employee noticed it still was not back up in May. Some hackers accessed the server and used the space there to store some movies, but the medical practice director said patients do not need to worry. A call center has been established for patients with questions, and anyone affected is being offered free credit monitoring for the next year. Source: <http://www.localnews8.com/news/28735650/detail.html>

TRANSPORTATION

Nothing Significant to Report

UNCLASSIFIED

UNCLASSIFIED

WATER AND DAMS

Nothing Significant to Report

NORTH DAKOTA 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; 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