

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

Company fined \$1.5M for disposal violations. North Dakota's Industrial Commission assessed a record \$1.525 million fine July 18 against the well drilling company, Halek Operating ND LLC of Dickinson, for putting Stark County drinking water at risk by illegally dumping more than 800,000 gallons of salt water waste into a former oil well. The State Department of Mineral Resources regulates the oil and gas industry and is overseen by the commission. The man who authorities say ordered the illegal dumping faces a felony charge of violating disposal rules, with a possible 5-year prison term. At the man's direction, workers tampered with a salt water disposal well that had failed a State inspection so it would pass a resinspection. The deception took place "literally in the middle of the night," and was discovered shortly afterward, officials said. They said the fine was the largest regulatory penalty ever for violating the commission's waste disposal rules, and the first time anyone was prosecuted under them. Additional tests are needed to see if the incident caused drinking water contamination. Officials said the company used cement that was inadequate to seal off the hole of the salt water disposal well, which was necessary to prevent the brine from leaking into nearby drinking water. Authorities believe at least 20,000 barrels of brine was illegally dumped. Source:

<http://www.sfgate.com/business/article/Company-fined-1-5M-for-disposal-violations-3717257.php>

REGIONAL

(Minnesota) Explosive device found, detonated near Milaca, Minn., shopping center. Police investigated an explosive device near a shopping center in Milaca, Minnesota. The device, a bomb containing nails, gun powder, and kerosene, was discovered during a traffic stop July 17. The suspect was pulled over twice and a K-9 officer was called to search the vehicle after the suspect was pulled over the second time and gave his consent. In the search, police found an explosive device and possible burglary tools. The suspect was then taken into custody. The Minnesota State Patrol, along with three other law enforcement agencies, closed off the street after employees of Thrivent Financial, Maple Ridge Mall, Dairy Queen, Barbara Jean's, Holiday, and Subway were informed that a bomb threat had been made. Officers evacuated the area. The area was reopened after about 5 hours. The Mille Lacs County sheriff said the suspect apparently intended to attempt suicide by using the explosive device inside his vehicle, but it is unknown where he likely would have struck. Source:

<http://www.myfoxtwincities.com/story/19045400/car-bomb-threat-at-dairy-queen-in-milaca-minn>

(Montana; Colorado) Missed cantaloupe listeria strain tied to man's death; new crop in stores. A previously unidentified strain of listeria from the 2011 deadly cantaloupe outbreak was linked to the death of a Montana man, NBC News reported July 18. The new strain was collected from cut cantaloupe in a home refrigerator in September 2011, at the start of the listeria outbreak that eventually sickened 146 people and led to at least 30 deaths and one miscarriage. However, Colorado health officials did not send the sample to federal officials for 10 months because it did not match strains from any known victims in that State. When they did send it to

UNCLASSIFIED

UNCLASSIFIED

the federal PulseNet monitoring program in June, it turned out to be identical to a rare strain of listeria detected in a Montana victim who died in January. That increases the number of strains in the 28-State outbreak to 5, up from the 4 strains responsible for most of the illnesses, said an epidemiologist at the Centers for Disease Control and Prevention (CDC). It also adds the man to the CDC's roster of cases, bringing the tally to 147, though it is not yet clear whether his death can be counted in the total. Source:

http://vitals.msnbc.msn.com/_news/2012/07/17/12794988-missed-cantaloupe-listeria-strain-tied-to-mans-death-new-crop-in-stores?lite&_utma=14933801.1290672222.1342454516.1342538156.1342619832.5&_utmb=14933801.1.10.1342619832&_utmc=14933801&_utmz=-&_utm

(South Dakota) South Dakota governor activates State Drought Task Force. South Dakota's governor activated the State Drought Task Force July 17, to monitor worsening drought conditions across much of the State. The group will coordinate the exchange of drought information among government agencies and agriculture, fire, and water-supply organizations. The information exchange is the key to monitoring the development and seriousness of the drought. The task force will also monitor the impact of drought on economic sectors of the State. Officials with the South Dakota Department of Agriculture, the State Office of Emergency Management, and South Dakota State University Cooperative Extension Service have been tracking drought conditions for several weeks. In addition, those agencies have worked with local officials and the U.S. Department of Agriculture's Farm Service Agency on the agricultural disaster declaration process, including pursuit of options to allow haying and grazing on land enrolled in the Conservation Reserve Program. Source:

<http://www.kcautv.com/story/19049820/south-dakota-governor-dennis-daugaard-activates-state-drought-task-force>

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Utility takes out Fukushima nuke fuel rods. A crane removed two rods packed with nuclear fuel from Japan's Fukushima Dai-Ichi nuclear plant July 18, the beginning of a process to deal with a remaining risk of more radiation escaping from the stricken plant. All of the 1,535 rods next to reactor No. 4 must eventually be removed from a spent-fuel pool to safer storage — an effort expected to take through the end of 2013, according to the Japanese government. The pool's building was destroyed by explosions from the multiple meltdowns that followed a massive earthquake and tsunami in March 2011. The pool is not protected by thick containment vessels like the core fuel in the plant's three other reactors. The plant's operator intends to remove the rods one-by-one to deal with the risk of radiation contamination to surrounding areas. Source:

<http://m.fox16.com/display/682/story/347d4c4fe8231e2146c185956bf00dee>

UNCLASSIFIED

BANKING AND FINANCE INDUSTRY

Criminals circumvent fraud detectors with real-time credential theft. Trusteer researchers found that cyber-criminals were employing new tactics to circumvent the risk analytics engines used by banks to detect financial fraud, SecurityWeek reported July 18. Criminals intercept a complete set of log-in credentials, block legitimate users from accessing the account, and log into a compromised account before the one-time password expires, Trusteer's CTO wrote in a blog post. By tricking users into entering the one-time password and blocking log-in attempts to the site, criminals circumvent the risk analytic tools used by banks to detect fraudulent behavior. The engines identify theft by looking for multiple devices simultaneously logged into a single account and successive logins from locations that are geographically too far apart. Malware intercepts the credentials and then shows users a page claiming the site is temporarily down, allowing the criminal to log in using the one-time password without triggering any alarms at the bank. Source: <http://www.securityweek.com/criminals-circumvent-fraud-detectors-real-time-credential-theft>

SMS, email, and phone call floods used by fraudsters to hide illegal money transfers.

Cybercriminals have come up with a new way of ensuring banks can not alert customers when fraudulent high-value transactions are taking place using mass emails, mass SMSs, and phone call floods, Softpedia reported July 18. When a bank requests confirmation of an unusual transfer via SMS, phone call, or email, cybercriminals will block those lines of communication by flooding them with spam messages. For instance, if the bank usually sends the confirmation notice via email, the crooks would flood the victim's email address with thousands of emails, making it almost impossible to find the one important message. Krebs On Security stumbled upon a number of tools – advertised on underground forums – that could easily perform these tasks. Prices for such tools were found to be low. For instance, for flooding a single email account with 25,000 emails, the customer pays \$25. For one day of flooding one phone number – service available for any country and any operator – the price was \$20. Mass SMS sending was even cheaper. For the price of \$5 fraudsters can send 100 text messages. Source: <http://news.softpedia.com/news/SMS-Email-and-Phone-Call-Floods-Used-by-Fraudsters-to-Hide-Illegal-Money-Transfers-281882.shtml>

Report: HSBC allowed money laundering that likely funded terror, drugs. A “pervasively polluted” culture at HSBC allowed the bank to act as financier to clients moving shadowy funds from the world's most dangerous and secretive corners, including Mexico, Iran, Saudi Arabia, and Syria, according to a U.S. Senate report issued July 16. The report, which came ahead of a Senate hearing July 17, said large amounts of Mexican drug money likely passed through the bank. HSBC's U.S. division also provided money and banking services to some banks in Saudi Arabia and Bangladesh believed to have helped fund al-Qa'ida and other terrorist groups, according to Al-Jazeera. While the British bank's problems have been known for nearly a decade, the Senate probe detailed just how sweeping the problems have been, both at the bank and at the Office of the Comptroller of the Currency (OCC), a top U.S. bank regulator that the report said failed to properly monitor HSBC. The study said the OCC failed to crack down on the bank despite multiple red flags, allowing money laundering issues “to accumulate into a

UNCLASSIFIED

massive problem.” Source: <http://bottomline.msnbc.msn.com/news/2012/07/17/12783850-report-hsbc-allowed-money-laundering-that-likely-funded-terror-drugs?>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

FDA says controversial plastic chemical BPA no longer allowed in baby bottles and sippy cups.

The federal government announced July 17 that baby bottles and sippy cups can no longer contain the chemical bisphenol-A, or BPA. The U.S. chemical industry’s chief association, the American Chemistry Council, had asked the Food and Drug Administration (FDA) to phase out rules allowing BPA in those products in October 2011, after determining that all manufacturers of bottles and sippy cups had already abandoned the chemical due to safety concerns. It is illegal for companies to use substances not covered by FDA rules. An FDA spokesman said however, that the agency continues to support the safety of BPA for use in products that hold food. The chemical industry’s request may help curb years of negative publicity from consumer groups and head off tougher laws that would ban BPA from other types of packaging.

Legislation introduced in Congress would ban BPA nationwide in all canned food, water bottles, and food containers. Chemical makers maintain the chemical is safe for food and drink uses.

Source: http://www.washingtonpost.com/business/industries/fda-says-controversial-plastic-chemical-bpa-no-longer-allowed-in-baby-bottles-and-sippy-cups/2012/07/17/gJQA1cg3qW_story.html

Indictment: 2 tried to send U.S. materials to Iran for nuclear program. A federal grand jury indicted two men, one from Iran and the other from China, on charges of conspiring to send materials from the United States to Iran for the purpose of enriching uranium, the U.S. Justice Department said July 13. Using a Chinese company as a go-between to avoid trade sanctions, the men tried for 3 years to obtain U.S. materials, such as high-strength steel, that could be used in an Iranian nuclear program, the department said. The Iranian citizen was arrested in May in the Philippines, while the other man remains at large, the department said. The two men succeeded in illegally exporting lathes and nickel-alloy wire from the United States to China and then to Iran around June 2009, according to the indictment. The Iranian man allegedly also began talking with an undercover U.S. federal agent in 2009, including in emails in which he tried to acquire radioactive source material. The emails continued into 2011, the indictment said. Source: <http://usnews.msnbc.msn.com/news/2012/07/13/12727005-indictment-2-tried-to-send-us-materials-to-iran-for-nuclear-program?lite>

COMMERCIAL FACILITIES

Security increased at movies following massacre. Around the country, some moviegoers noticed increased security at July 20 showings of the new Batman movie, in the wake of a July 20 shooting rampage at a theater in Colorado that left 12 people dead. Two police officers were stationed outside a theater in New York City’s Times Square July 20, where showings of The Dark Knight Rises started every 20 minutes. At a theater in downtown Washington, D.C., moviegoers trickled into showings. Theater employees searched patrons’ bags and purses while taking their tickets. Staff members at a Philadelphia theater said the extra security that was in

UNCLASSIFIED

UNCLASSIFIED

place was normal for big movies, and not a result of the shooting in Colorado. Source: <http://www.myfoxlubbock.com/news/national/story/NYPD-provides-coverage-at-movie-theaters/UtyqwzTf6US6kjqugYxnVg.csp>

COMMUNICATIONS SECTOR

Nothing Significant to Report

CRITICAL MANUFACTURING

Ford recalls 2013 Escape because fuel lines can crack and cause engine fires. Ford told owners of one version of the 2013 Ford Escape not to drive the sport utility vehicles (SUV) until dealers can fix fuel lines that can crack and spill gasoline, causing engine fires, the Associated Press reported July 19. The company issued the unusual warning and said it is recalling 2013 Escapes equipped with 1.6-liter four-cylinder engines. Dealers will pick up the Escapes and drop off a loaner car that customers can use until the repairs are finished. The company is hoping to ship parts and get all the SUVs repaired in the next 2 weeks. Ford said it has three reports of fires: Two at the factory and one while a customer was driving an Escape. The recall affects 11,500 Escapes in the United States and Canada. Only 4,800 have been sold to customers. The rest are on dealer lots and will be fixed before they are sold, a Ford spokeswoman said. Source: http://www.washingtonpost.com/business/ford-recalls-2013-escape-because-fuel-lines-can-crack-and-cause-engine-fires/2012/07/19/gJQA0EqZvW_story.html

Honda recalls 172,000 crossovers, luxury sedans. Honda announced the recall of 166,000 2012 CR-V and 6,200 2013 Acura ILX vehicles due to a problem with the vehicles' door latches that could cause a door to open while driving, the Detroit Bureau reported July 19. According to a statement from the company, "Simultaneous operation of the driver's or passenger's inner door handle and either the manual or power door lock may result in the inner door handle release cable becoming partially disengaged. When this occurs the door may not latch when closed and/or the door may latch and close, but then open when the door locks are operated; either case may result in the affected door opening unexpectedly." Source: <http://bottomline.msnbc.msn.com/news/2012/07/19/12832985-honda-recalls-172000-crossovers-luxury-sedans?lite>

Feds probe Ford Escapes for sticky throttles. Government safety regulators were investigating complaints that throttles can stick on older-model Ford Escape and Mazda Tribute sport utility vehicles (SUV) and cause them to crash, the Associated Press reported July 18. The probe by the National Highway Traffic Safety Administration affects 730,000 SUVs from the 2001 to 2004 model years that are powered by V-6 engines. The safety agency said it has received 99 complaints from owners of the SUVs alleging 13 crashes, 9 injuries, and 1 death caused by the problem. The throttles on the SUVs can fail to return to idle when the driver takes his foot off the gas pedal, according to agency documents. Sixty-eight of the complaints were about the Escape, and 31 involved the Tribute, a nearly identical vehicle made by Ford for Mazda. Investigators are looking into whether the sticky throttles could have been caused by repairs

UNCLASSIFIED

UNCLASSIFIED

made as part of a 2004 recall of the same vehicles. About 590,000 of the vehicles were recalled in December of 2004 to fix an accelerator cable defect, and the documents said the repairs could have damaged the cruise control cable. Source:

<http://www.manufacturing.net/news/2012/07/feds-probe-ford-escapes-for-sticky-throttles>

NHTSA recall notice - Nissan Juke rear seat back striker welds. Nissan announced July 17 the recall of 11,076 model year 2012 Juke vehicles manufactured from February 3, 2012 through May 26, 2012. Due to an incomplete weld penetration, the rear seat back striker may partially separate in a crash. In the event of a crash, the rear seat back may not be secured, increasing the risk of injury to the rear seat occupants. Nissan will notify owners, and dealers will replace the affected seat back strikers. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld_ID=12V328000&summary=true&prod_id=1436771&PrintVersion=YES

DEFENSE/ INDUSTRY BASE SECTOR

More problems for F-22 beyond mysterious oxygen loss issue. July 16, CNN reported that two recent in-flight emergencies involving troubled oxygen systems in the F-22 “Raptor” are unrelated to other breathing problems pilots experienced for more than a year when flying the plane, according to U.S. Air Force officials. The Air Force is investigating why a number of F-22 pilots experienced a mysterious loss of oxygen while in the air, causing dizziness and confusion known as hypoxia, since spring 2011. However, two recent incidents related to the oxygen system are considered regular mechanical issues not connected to the oxygen deprivation investigation, according to a spokesman for the Air Force’s Air Combat Command. Air Force officials labeled the number of unexplained F-22 breathing incidents as “cause unknown,” while labeling the two recent incidents as “cause known.” In a response to a CNN inquiry, the spokesman sent information on what Air Force initial investigations found in the two recent incidents. He said the mechanical issues were “not specific to the F-22 aircraft.” One of the incidents, an oxygen system malfunction July 6, is still under investigation by the Air Force and the plane remains grounded, according to the Air Force information provided by the spokesman, but the incident is still listed as a “cause known” problem. Source:

<http://security.blogs.cnn.com/2012/07/16/more-problems-for-f-22-beyond-mysterious-oxygen-loss-issue/>

EMERGENCY SERVICES

(California) Redwood City police use video-text chat. A new pilot program — the first in the nation, the department said — that allows residents to chat with an officer online to deal with anything except a life-threatening emergency, has debuted in Redwood City, California, the San Francisco Chronicle reported July 17. “The beauty of this program is that residents could do this from their homes, from school, from work, anywhere that they have a laptop or desktop with something as simple as a camera on it,” said the police chief, who came up with the idea. Anyone, not just Redwood City residents, can chat with an officer, and they can do so by audio, video, or via texts on a computer screen. The chats are not recorded, and users cannot be

UNCLASSIFIED

UNCLASSIFIED

traced. The program is usually in session from 9 a.m. to 5 p.m., Monday through Thursday. The department plans to expand the program to weekends and evenings and could add bilingual officers if there is a need, police said. Source: <http://www.sfgate.com/crime/article/Redwood-City-police-use-video-text-chat-3714948.php>

Hacker opens high security handcuffs with 3D-printed and laser-cut keys. In a workshop July 13, at the Hackers On Planet Earth conference in New York City, a German hacker and security consultant demonstrated a looming problem for handcuff makers hoping to restrict the distribution of the keys that open their cuffs: With plastic copies he cheaply produced with a laser-cutter and a 3D printer, he was able to open handcuffs built by the German firm Bonowi and the English manufacturer Chubb, both of which attempt to control the distribution of their keys to keep them exclusively in the hands of authorized buyers such as law enforcement. The demonstration highlighted a unique problem for handcuff makers, who design their cuffs to be opened by standard keys possessed by every police officer in a department, so that a suspect can be locked up by one officer and released by another, said the security consultant. Unlike other locks with unique keys, any copy of a standard key will open a certain manufacturer's cuff. Source: <http://www.forbes.com/sites/andygreenberg/2012/07/16/hacker-opens-high-security-handcuffs-with-3d-printed-and-laser-cut-keys/>

ENERGY

McAfee report highlights critical need for improved energy grid security. McAfee announced a report detailing the thoughts of industry leaders on the state of energy security July 18. The report, Getting Smarter About Smart Grid Cyberthreats, looks at how legacy smart grids are vulnerable to attack and how security must be built into these critical systems. The electrical power grid is the backbone on which everything else depends on, the report stated. It noted a cybercriminal could debilitate a major city by a single targeted attack on the energy grid and compromise anything from the lights and appliances in homes, to heart monitors in hospitals, to air defense systems. The most prevalent cyberthreat reported by the global energy sector is extortion, the study found. Criminals gain access to a utility's system, demonstrate that they are capable of doing damage, and demand a ransom. The report said additional threats include espionage and sabotage, all with the goal of financial gain, data theft, and shutting down facilities. Source: <http://www.mcafee.com/us/about/news/2012/q3/20120718-01.aspx>

Oil companies spring a leak, courtesy of Anonymous. Five top multinational oil companies have been targeted by members of Anonymous, who published about 1,000 email addresses for accounts belonging to the firms, as well as hashed and unencrypted passwords, Wired reported July 16. The hacks, against Shell, Exxon, BP, and two Russian firms — Gazprom and Rosneft, were conducted as digital protests against drilling in the Arctic, a practice critics say has contributed to the melting of the ice caps. The hackers used some of the stolen credentials to add signatures to Greenpeace's "Save the Arctic" petition. The latest disclosure follows an earlier one in June in which credentials for Exxon were released. The hackers said then that they obtained the credentials not through a vulnerability in Exxon's network, "but just because of the mistake of their webmaster!", suggesting an administrator misconfigured something

UNCLASSIFIED

UNCLASSIFIED

related to the Web site. The hackers noted in their post that they are not associated with Greenpeace, they just support its cause. Source:

<http://www.wired.com/threatlevel/2012/07/oil-companies-hacked/>

FOOD AND AGRICULTURE

Widespread drought is likely to worsen. The drought that has settled over more than half of the continental United States is the most widespread in more than half a century, and it is likely to grow worse, the New York Times reported July 19. The latest outlook released by the National Weather Service July 19 forecasts increasingly dry conditions over much of the nation's breadbasket, a development that could lead to higher food prices and shipping costs as well as reduced revenues in areas that count on summer tourism. About the only relief in sight was tropical activity in the Gulf of Mexico and the Southeast that could bring rain to parts of the South. As of July 15, more than half of the corn in seven States was in poor or very poor condition, according to the Department of Agriculture. In Kentucky, Missouri, and Indiana, that figure is above 70 percent. Overall, only 31 percent of the nation's corn is in good to excellent condition, compared with 66 percent at the same time in 2011. The withering corn has increased feed prices and depleted available feeding land, putting stress on cattle farmers. A record 54 percent of pasture and rangeland — where cattle feed or where hay is harvested for feeding — was in poor or very poor condition, said the Department of Agriculture. Many farmers have been forced to sell their animals. Because feed can account for nearly half of a cattle farmer's costs, consumers could see a rise in the price of meat and dairy products, experts said. Source: <http://www.nytimes.com/2012/07/20/science/earth/severe-drought-expected-to-worsen-across-the-nation.html?pagewanted=all>

More than 1,200 counties declared disasters. As of July 18, 1,207 counties in 29 States were declared disaster areas eligible for disaster assistance by farmers and ranchers. The total included 39 counties added to the list the week of July 16 by the U.S. Department of Agriculture (USDA) because of drought and excessive heat. The USDA Drought Monitor reported 61 percent of the continental United States was in a moderate to exceptional drought and thoughts are that more area will fall in at least moderate drought after the current heat wave in a large portion of the nation. The additional counties designated disaster areas are in the States of Arkansas, Georgia, Indiana, Mississippi, New Mexico, Tennessee, Utah, and Wyoming. Source: <http://www.agprofessional.com/news/More-than-1200-counties-declared-disasters-163011306.html>

Drought in U.S. reaching levels not seen in 50 years, pushing up crop prices. A drought gripping the Corn Belt and more than half of the United States has reached proportions not seen in more than 50 years, the government reported July 16, increasing crop prices and threatening to drive up the cost of food. The week of July 9, the Agriculture Department declared more than 1,000 counties in 26 States as natural-disaster areas. About 55 percent of the continental United States is now designated as in moderate drought or worse, the largest percentage since December 1956, said the National Climatic Data Center. "The drought could get a lot worse before it gets better," said the chief economist at the Agriculture Department.

UNCLASSIFIED

UNCLASSIFIED

The Agriculture Department July 16 said 38 percent of the U.S. corn crop was in poor or very poor condition, up from 30 percent from the previous week. Source:

http://www.washingtonpost.com/business/economy/drought-in-us-reaching-levels-not-seen-in-50-years-pushing-up-corn-prices/2012/07/16/gJQA01SopW_story.html?hpid=z5

Food genome database planned. The next step in the ongoing U.S. effort to limit outbreaks of food-borne illnesses, which are occurring about 1,000 times per year, is a new collaboration involving the U.S. Food and Drug Administration (FDA), the University of California, Davis, Agilent Technologies Inc., and the Centers for Disease Control and Prevention to create a free, public database of 100,000 food-borne pathogen genomes. Once it is established about 5 years from now, it will enable faster identification of bacteria responsible for outbreaks, Occupational Health & Safety reported July 16. FDA announced the collaboration July 12, saying the typical public health response time in outbreaks will be “days instead of weeks.” Allowing open access to the database will foster the creation of tests to identify bacteria in a sample “within a matter of days or hours, significantly faster than the approximately one week it now takes between diagnosis and genetic analysis,” it said. FDA is providing more than 500 completed Salmonella genome draft sequences and thousands more important food pathogen strains for sequencing; the agency’s scientists also will help with guiding the project and providing technical assistance. The database will include the genomes of important pathogens such as Salmonella, Listeria, and E. coli. Source: <http://ohsonline.com/articles/2012/07/16/food-genome-database-planned.aspx?admgarea=ht.FoodSafety>

Mandatory pig traceability coming soon to Canada. Traceability is soon going to be a requirement for pigs raised for slaughter in Canada, Food Safety News reported July 17. The Canadian Food Inspection Agency wrote new rules designed to require pork producers to identify all farmed pigs and farmed wild boars using approved methods and to record and report all movements of pigs from birth or import to slaughter or export. The Government of Canada said mandatory traceability for pigs was developed after consultations with the swine industry, provinces and territories, and other stakeholders. Canada already has mandatory identification systems in place for cattle, bison, and sheep. Source: <http://www.foodsafetynews.com/2012/07/mandatory-pig-traceability-coming-soon-to-canada/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Virginia; Washington, D.C.) **Mass. man admits guilt in plot to blow up Pentagon.** A Massachusetts man pleaded guilty July 20 to his role in a plot to use remote-controlled model planes packed with explosives to blow up the Pentagon and U.S. Capitol in Washington, D.C. He pleaded guilty to attempting to provide material support to terrorists and attempting to damage and destroy federal buildings by means of an explosive. He was arrested in 2011 after federal employees posing as al Qa’ida members delivered materials he requested, including grenades, machine guns, and plastic explosives. In court documents, authorities said he

UNCLASSIFIED

UNCLASSIFIED

traveled to Washington to do surveillance and rented storage space to work on the planes in Framingham, Massachusetts. The man was accused of planning to use three remote-controlled planes measuring 60 to 80 inches in length and capable of speeds greater than 100 mph. Each plane, guided by GPS, was to be packed with 5 pounds of explosives. Under a plea agreement, prosecutors and the defense will request a 17-year sentence on charges that carry a combined maximum of 35 years in prison. Source:

<http://www.google.com/hostednews/ap/article/ALegM5iATLisgYEaCGKW8ycnGt-hm6XRrw?docId=bdd8fa3e886a44838e31d99505a191a1>

Agencies face 'hodge-podge' guidance on security clearances. According to a July 12 report by the U.S. Government Accountability Office (GAO), the Director of National Intelligence (DNI) failed to provide agencies with clear guidelines about which positions require clearances. Further, the DNI has not created guidance requiring agencies to periodically review those designated positions. In the absence of official guidelines from the DNI's office, agencies have made do with an Office of Personnel Management tool designed to determine the sensitivity level of a position. Used alone, however, the tool is not meant to determine if a position actually requires a clearance, said the director of GAO's defense capabilities and management issues. "In the absence of clearly defined policy from the DNI and the lack of collaborative input into the tool's design," the GAO report stated, "officials explained that they sometimes had difficulty in using the tool to designate the sensitivity level of national security positions." Similarly, agencies do not have consistent guidelines for reviewing and validating existing security clearances to ensure clearances are kept to a minimum. Source:

<http://www.federalnewsradio.com/520/2945512/Agencies-face-hodge-podge-guidance-on-security-clearances>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Report: Bandwidth-burning malware among biggest consumer threats. A new malware report indicates Android malware samples grew three-fold in the second quarter of 2012, and that 1 in every 140 devices connected to mobile networks was infected at some point. About 14 percent of household networks were hit by malware in the spring, with a 50 percent increase in high-level bots, trojans, and backdoors, according to the Q2 2012 Malware Report from Kindsight Security Labs. Among the biggest threats to consumers was the ZeroAccess botnet, which grew to more than 1.2 million super nodes resulting in ad-click fraud that at one point used bandwidth equivalent to 45 monthly movie downloads per subscriber. Source:

http://threatpost.com/en_us/blogs/report-bandwidth-burning-malware-among-biggest-consumer-threats-071912

Phishing websites reach all-time high. The number of phishing Web sites detected reached an all-time high earlier in 2012, a sign that making fake Web sites spoofing real ones is still a lucrative trade for cyber criminals. In its latest report, the Anti-Phishing Working Group (APWG) said 56,859 phishing sites were detected in February, beating the previous record high in August 2009 by nearly 1 percent. APWG is a nonprofit consortium composed of banks, security vendors, and others with a stake in tracking cybercrime trends. Phishing sites are Web sites that

UNCLASSIFIED

UNCLASSIFIED

look nearly identical to legitimate ones and often mimic known brands. Leveraging the trust users put in legitimate companies, cyber criminals trick victims into divulging logins, passwords, and other sensitive data. The APWG noted in its report that the increase in the number of phishing sites was in part due to new technology that it began using earlier in 2012 to detect fake sites. More than 38 percent of the fake sites were related to financial services, said the report. The second most spoofed market vertical was payment services, followed by retail and other service sites. The sites spoofed 392 brands, also a new record. Source: http://www.computerworld.com/s/article/9229398/Phishing_websites_reach_all_time_high

Researchers say they took down world's third-largest botnet. July 18, computer security experts took down Grum, the world's third-largest botnet, a cluster of infected computers used by cyber criminals to send spam to millions of people. Grum, computer security experts said, was responsible for roughly 18 percent of global spam, or 18 billion spam messages a day. Computer security experts blocked the botnet's command and control servers in the Netherlands and Panama July 17. However, later that day, Grum's architects set up seven new command and control centers in Russia and Ukraine. FireEye, a computer security company in California, said it worked with its counterparts in Russia and with SpamHaus, a British organization that tracks and blocks spam, to take down those command and control centers the morning of July 18. Source: <http://bits.blogs.nytimes.com/2012/07/18/cybersecurity-researchers-say-they-took-down-worlds-third-largest-botnet/>

Android malware steals location data from mobile devices. BitDefender Labs discovered Android malware that regularly broadcasts the location of the infected mobile device to a remote server. What the malware creators intend to do with the privacy-invading information is unclear. The application operates in the background and appears on the smartphone or tablet as an icon with the word "store" written on it. The store icon is apparently meant to fool the device user into thinking that it is only an e-commerce app, according to Bitdefender. In actuality, the malware broadcasts latitude and longitude of the device, as well as the name of the wireless carrier. It also attempts to enable the device's Wi-Fi connection and scan for access points. All of the data is transmitted to the remote server via the device's Internet connection. The spyware has no user interface and transmits location information every few seconds. Because the malware runs so effectively in the background, Bitdefender believes it will eventually be bundled with other apps. Source: http://www.computerworld.com/s/article/9229328/Android_malware_steals_location_data_from_mobile_devices

Android malware is booming. Trend Micro's January prediction that 11,000 pieces of Android malware will be detected by June of 2012 proved completely inaccurate, as the number of malicious applications in the wild for Google's mobile operating system exploded and now is at more than 25,000. Forty-eight percent of these malicious apps are premium service abusers, followed by 22 percent that are adware, and 21 percent that are data stealers. Malicious downloaders are offered in 19 percent of cases, while rooters, click fraudsters, and spying tools are at the bottom of the ladder. The apps are pushed onto users through third-party online stores and even the official Google Play app store. Usually, they masquerade as legitimate and

UNCLASSIFIED

UNCLASSIFIED

popular software such as Angry Birds, Skype, and Instagram. This unexpected boom in Android malware made the researchers revise their expectations — they believe there may be a total of 129,000 different malicious apps by the end of 2012. Source: http://www.net-security.org/malware_news.php?id=2192&utm

ICS-Alert-12-195-01—Tridium Niagara directory traversal and weak credential storage vulnerability. Two independent security researchers notified the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) of a directory traversal and weak credential storage vulnerability with proof-of-concept exploit code for Tridium Niagara AX Framework software. According to their research, the vulnerabilities are exploitable by downloading and decrypting the file containing the user credentials from the server. ICS-CERT is coordinating with the researchers and Tridium. Original attempts to coordinate vulnerability information were unsuccessful and ICS-CERT, in coordination with the researchers, was planning a release of the vulnerability data. However, recent communications from Tridium indicated they were working on a solution, resulting in the delayed release of this Alert so mitigations/patches could be prepared. July 12, a public report came out detailing the vulnerabilities and as a result, ICS-CERT shortened its release schedule and issued this Alert to warn of the unpatched vulnerabilities. Tridium released a security alert with instructions on how to implement interim mitigations. Tridium stated they are testing a software update that will resolve the vulnerabilities. ICS-CERT will issue an Advisory when the software update is available. According to the Tridium Web site, more than 300,000 instances of Niagara AX Framework are installed worldwide in applications that include energy management, building automation, telecommunications, security automation, machine to machine, lighting control, maintenance repair operations, service bureaus, and total facilities management. Source: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-195-01.pdf

NVIDIA hackers publish user data. Late the week of July 9, NVIDIA confirmed the database for its forums Web site was broken into by unauthorized third parties, with data from more than 400,000 registered users affected. A hacker group calling itself “Team Apollo” has now claimed responsibility for the breach which caused NVIDIA to take the site down. As proof, they published email addresses and password hashes for about 800 users from the database on Pastebin, with more, apparently, to follow. If the data proves to be genuine, NVIDIA’s statement that the password hashes were salted would be contradicted: the database excerpt includes the hash b018f55f348b0959333be092ba0b1f41 three times in the list, the result of md5(‘nvidia123’). In addition, the hackers stated NVIDIA’s online store was broken into, which NVIDIA did not mention to The H’s associates at heise Security. The hacker group said the break-in occurred “a few weeks ago.” Source: <http://www.h-online.com/security/news/item/NVIDIA-hackers-publish-user-data-1643038.html>

Trend Micro confirms Yahoo! Mail flaw possible cause of “Android botnet”. Researchers from mobile security firm Lookout identified a security hole in the Yahoo! Mail application for Android, which they believed to be responsible for the so-called mobile spam botnet. July 16, Trend Micro experts confirmed the existence of the flaw. They could not precisely say if the vulnerability is in fact responsible for the spam sent out from mobile phones, but the fact that

UNCLASSIFIED

UNCLASSIFIED

they independently appoint the same weakness as a possible cause makes this scenario more plausible. The weakness discovered by the researchers allows an attacker to steal a user's Yahoo! cookies. "This bug stems from the communication between Yahoo! mail server and Yahoo! Android mail client. By gaining this cookie, the attacker can use the compromised Yahoo! Mail account to send specially-crafted messages. The said bug also enables an attacker to gain access to user's inbox and messages," a mobile threats analyst said. Currently, the fix for the issue is being coordinated with Yahoo! and the researchers promise a more technical analysis, but in the meantime, users must be extra cautious when receiving shady pharmacy advertisements that appear to be sent from Android devices via Yahoo! Mail. Source: <http://news.softpedia.com/news/Trend-Micro-Confirms-Yahoo-Mail-Flaw-Possible-Cause-of-Android-Botnet-281493.shtml>

NATIONAL MONUMENTS AND ICONS

Nothing Significant to Report

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

CDC: Whooping cough rising at alarming rate in U.S. Nearly 18,000 cases of whooping cough have been reported in 2012 — more than twice the number seen at this point in 2011, the Centers for Disease Control and Prevention said July 19. At this pace, the number for the entire year will be the highest since 1959, when 40,000 illnesses were reported. Nine children have died, and health officials called on adults — especially pregnant women and those who spend time around children — to get a booster shot as soon as possible. Health investigators are trying to figure out what is causing the increase, with theories including better detection and reporting of cases, some sort of evolution in the bacteria that cause the illness, or shortcomings in the vaccine. The original vaccine that had been given to young children for decades was replaced in the late 1990s following concerns about rashes, fevers, and other side effects. For about 25 years, fewer than 5,000 cases were reported annually. The numbers started to climb again in the 1990s. In both 2004 and 2005, cases surpassed 25,000. The numbers dipped for a few years but jumped to more than 27,000 in 2010, the year California saw an especially bad epidemic. Experts believe whooping cough occurs in cycles and peaks every 3 to 5 years. Source: <http://www.news-gazette.com/news/health/health-care/2012-07-20/cdc-whooping-cough-rising-alarming-rate-us.html>

(New York) Whooping cough cases on rise, New York urges vaccinations. New York's Health Department July 18 reported a sharp spike in cases of whooping cough. Preliminary figures found 970 cases so far in 2012 of the highly contagious disease pertussis, or whooping cough. In all of 2011, there were 931 cases reported in New York. By June, the number of reported cases in the United States in 2012 was nearly 44 percent higher than the same period in 2011,

UNCLASSIFIED

UNCLASSIFIED

according to the U.S. Centers for Disease Control and Prevention (CDC). New York is one of more than a dozen U.S. States reporting a greater than three-fold increase in reported cases of the whooping cough since 2011, according to the CDC. Health officials attributed the rise in whooping cough to the cyclical nature of the disease where the number of reported cases hits a peak every 3 to 5 years. Source: <http://www.foxnews.com/health/2012/07/19/whooping-cough-cases-on-rise-new-york-urges-vaccinations/>

(Washington) State surpasses 3,000 whooping cough cases for 2012. More than 3,000 cases of whooping cough have been diagnosed in Washington State so far in 2012, according to data compiled by the Washington Department of Health (WDH). That number is far in excess of the 219 cases diagnosed in the same period in 2011. A total of 131 new cases were documented in Washington between July 8-14, bringing the 2012 total to 3,014. The hardest hit group is children between the ages of 10 and 13. The Centers for Disease Control and the WDH planned a briefing on the epidemic to provide additional information on prevention resources July 19. Source: <http://www.krem.com/news/163021736.html>

Fed. panel supports Kan. biosecurity lab project. A government-backed committee of the National Research Council issued a report July 13 saying the United States would have adequate biosecurity protections even if plans for a proposed \$1.14 billion lab in Kansas are scaled back. The study looks at three options for the National Bio- and Agro-Defense Facility to be built in Manhattan near the Kansas State University campus. The DHS asked the council to review the threats of foreign animal disease, the capabilities needed to address such threats, and analyze options for building the lab as proposed or scaling back the size and scope. The first option would be to continue designing and constructing the new lab in Kansas, which would give the United States a large-animal lab with Level 4 security to handle such deadly diseases as foot and mouth. However, the costs for the project have escalated. The second option would be to scale back the size of the project and disperse research of diseases across the country. A third option, which would leave current research at Plum Island, New York, and rely on foreign labs to conduct research and deter threats, was rejected by the committee. Source: http://www.google.com/hostednews/ap/article/ALeqM5iJjsRjLiMf_mPfbGVFE-AAE1M2w?docId=6ce552a424324aa18b07da7d57723bcd

TRANSPORTATION

(Utah) Feds: Murder suspect tries to steal plane, crashes, then kills self. A murder suspect from Colorado Springs, Colorado, attempted to hot-wire a SkyWest Airlines regional jet at the airport in St. George, Utah, overnight, then crashed it into a fence before killing himself, federal law enforcement authorities said July 17. A pilot on leave from the regional carrier broke into the plane, which was parked at the airport in southwest Utah, authorities said. He got the plane started but clipped a wing before he got airborne and crashed into a fence. He then shot himself dead, authorities said. SkyWest said it was investigating how the man was able to gain access to the plane, which was sitting on the ramp at the St. George airport. Airport security and perimeter is the responsibility of the airport and local police, but must be approved by the federal Transportation Security Administration (TSA). The TSA said commercial airplane doors

UNCLASSIFIED

UNCLASSIFIED

are not locked when parked. Source:

<http://usnews.msnbc.msn.com/news/2012/07/17/12793149-feds-murder-suspect-tries-to-steal-plane-crashes-then-kills-self?lite>

(Michigan) Ambassador Bridge in Detroit open again after bomb threat. Traffic was reopened on the Ambassador Bridge July 17, a U.S.-Canada span that was closed for hours while authorities checked out a bomb threat July 16 on the U.S. side of the bridge in Detroit. There was a similar threat 4 days earlier to a nearby tunnel crossing. According to the Michigan Department of Transportation, traffic was at normal levels as rush hour approached July 17. Detroit police said someone called 9-1-1 saying a bomb would go off in 10 minutes. The call prompted authorities in Detroit and Windsor, Ontario, to halt all truck and car traffic across the bridge. The bridge was reopened July 17 after security sweeps failed to turn up any incendiary devices. Source:

http://www.mlive.com/news/detroit/index.ssf/2012/07/ambassador_bridge_in_detroit_o.html

(Michigan) Ambassador Bridge in Detroit open again after bomb threat. Traffic was reopened on the Ambassador Bridge July 17, a U.S.-Canada span that was closed for hours while authorities checked out a bomb threat July 16 on the U.S. side of the bridge in Detroit. There was a similar threat 4 days earlier to a nearby tunnel crossing. According to the Michigan Department of Transportation, traffic was at normal levels as rush hour approached July 17. Detroit police said someone called 9-1-1 saying a bomb would go off in 10 minutes. The call prompted authorities in Detroit and Windsor, Ontario, to halt all truck and car traffic across the bridge. The bridge was reopened July 17 after security sweeps failed to turn up any incendiary devices. Source:

http://www.mlive.com/news/detroit/index.ssf/2012/07/ambassador_bridge_in_detroit_o.html

A year after floods, shippers face low Miss. River. A year after the Mississippi River swelled to near-historic proportions and flooded farms and homes from Illinois to Louisiana, the level along the waterway's southern half is so low that cargo barges have run aground and their operators have been forced to lighten their loads, the Associated Press reported July 16. A major concern at Greenville, Mississippi, and other ports is that the entrance to the river could get too shallow. If that happens, barges could be forced to carry lighter loads to make it to the channel. Wide, sandy strips of shoreline usually invisible even in the low season are now exposed, shrinking the river's width and affecting the way tow captains navigate. With the river this low, the channels are shallower and narrower, presenting problems for barges loaded with coal, grain, iron, steel, sand, gravel, and more. They must reduce their loads to avoid bottoming out and take extra care not to collide when passing another string of barges in the thinner channel. Also, low water at docks and terminals makes it more difficult to load or unload material, as ships have trouble getting close enough to docks. Source:

<http://www.myrtlebeachonline.com/2012/07/16/2941450/a-year-after-floods-shippers-face.html>

FAA proposes fining Boeing \$13.5 million. The Federal Aviation Administration (FAA) July 13 proposed fining Boeing \$13.5 million for failing to meet a deadline to provide airlines with

UNCLASSIFIED

UNCLASSIFIED

instructions on how to prevent fuel tank explosions like the one that destroyed TWA Flight 800 off the coast of Long Island, New York in 1996, killing all 230 people on board. Boeing put the nitrogen generating systems the FAA wants on all planes it has built since August 2010. And since June 2008, the systems have gone on every 737. The nitrogen makes it harder for volatile gases to ignite. The FAA's penalty involves older 747s as well as the 757, which Boeing no longer makes. Both planes are flown by Delta, United, and Continental. The 757 is also flown by American Airlines and US Airways. In total, 383 U.S.-registered planes are affected by these delays, the FAA said. U.S. airlines, through the trade group Airlines for America, have asked the FAA to extend the deadlines for retrofitting their fleets, which fall in 2014 and 2017. The FAA said July 13 it would not issue a blanket extension but would consider extension requests by individual airlines for the 2014 deadline when they must retrofit half their fleets. The fine underscores the difficulty the agency has had prodding industry to comply with important safety regulations that can be complex or expensive to implement. Source: http://www.emissourian.com/news/state/article_cc66c41e-cf4b-11e1-aed1-0019bb2963f4.html

WATER AND DAMS

(Indiana) Entire state under water shortage warning. The Indiana Department of Homeland Security extended a water shortage warning to all 92 counties July 17 after placing less than half the state in that category a week ago. State officials asked for voluntary water conservation, specifically asking high-volume users to reduce the volume they use by 10-15 percent. If conditions worsen, the governor could declare an emergency and put mandatory rules into place. In central Indiana, Citizens Water draws from three reservoirs, all of which are down from their usual levels at this time of year. Morse Reservoir is down nearly 6 feet, Geist Reservoir and Eagle Creek are both nearly 2 feet below normal. Citizens said it will increase filtration at its Fall Creek treatment plant, which will enable it to reduce the amount being drawn from Morse Reservoir for its White River treatment plant. Source: <http://www.wishtv.com/dpp/news/indiana/entire-state-under-water-shortage-warning>

(Utah) Echo Dam gets a seismic facelift to prevent failure. A seismic overhaul of the aging Echo dam south of I-84 in Weber Canyon is the largest federal project of its kind in Utah, representing a 4-year, \$50 million effort, KSL 5 Salt Lake City reported July 16. When completed in late 2014, the earthquake safety modifications will meet or exceed federal standards, and the dam will no longer be rated at risk of catastrophic failure, by the U.S. Bureau of Reclamation. Excavation at the base of the dam began in June, and is 6 weeks ahead of schedule because of a warm spring and an early draw on the waters. Crews will remove 665,000 cubic yards of dirt down to bedrock at the downstream slope of the dam, using heavy equipment to gouge out a massive hole. A safety analysis found dirt at its foundation and underneath the spillway controls could liquefy in an earthquake. A seismic analysis shows a fault plane between Henefer and East Canyon Dam to the west capable of a 6.5-magnitude earthquake. Officials said a collapse of the dam would imperil all the communities downstream — Henefer, Morgan, Peterson, Stoddard, Uintah, and South Weber. Flood waters would reach the flatlands of Plain City, more than 50 miles away in Weber County. Once the hole is replaced

UNCLASSIFIED

UNCLASSIFIED

with the denser material, contractors will construct an earthen stability berm designed to buttress the dam. Another upstream berm will be constructed and compacted to further minimize the risk of any catastrophic failure. That project will begin in the fall as the reservoir levels continue to drop. Source: <http://www.ksl.com/?nid=960&sid=21284762>

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