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.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **7 Karlstad homes destroyed; wildfire contained.** Seven homes, including three mobile homes, were destroyed October 2 in Karlstad, Minnesota, after high winds fanned a wildfire that had been burning since September 30. The County 27 Fire was one of eight weekend fires that started burning the weekend of September 29 in Minnesota's Wannaska complex. The fire was estimated to have grown to about 4,720 acres October 2, according to the Minnesota fire marshal. That was nearly half of the estimated 9,800 acres consumed in the eight fires throughout the Wannaska complex. Other fires were near Fourtown, Goodridge, Greenbush, Lancaster, Middle River, and Thief River Falls. At least half of the Kittson County community of 800, including the Kittson Memorial Nursing Home and Assisted Living Center and Tri-County Public School, was evacuated October 2, the fire marshal said, but residents were allowed to return home before dark. School was canceled October 3 in Karlstad. An estimated 150 firefighters, Minnesota National Guard, and other agencies were on the scene. At least 16 fire departments assisted, said the fire marshal. Source: http://www.inforum.com/event/article/id/376169/group/news/

(Minnesota) **Xcel: Sherco power plant repairs could cost $200M.** Xcel Energy Inc. said it will cost as much as $200 million to repair the damage from a catastrophic turbine failure at Minnesota's largest power plant November 2011, the Associated Press reported October 3. The Sherco plant director said Xcel still has not determined exactly why the turbine at the plant in Becker broke up, sending debris and metal flying and sparking a fire. He said consultants are expected to finish the investigation at the end of this year. The director said most repair costs will be covered by insurance. He said Xcel and contractors are working around the clock to complete the repairs so Unit 3 can restart in the first quarter of 2013. Source: http://www.kttc.com/story/19724446/xcel-sherco-power-plant-repairs-could-cost-200m

(Minnesota) **Minneapolis shooter spared some, shot others; fifth victim dies.** The suspect who shot up a Minneapolis, Minnesota, sign-making business selected his targets carefully, walking past some employees while shooting others, police said September 28. The Minneapolis Police detailed the suspect's shooting rampage as a fifth victim died from wounds. The suspect later shot himself in the head, bringing the total number of victims of the September 27 attack to six. The suspect shot up Accent Signage Systems just hours after he was fired from the company. The chief said the suspect used a 9mm Glock semi-automatic pistol. Police who searched his home September 28 found an additional gun. The guns were purchased in 2011 and he had been practicing shooting them. Authorities found packaging for 10,000 rounds of ammunition in the house. Source: http://www.masoncountydailynews.com/news/national-news/40290-minneapolis-shooter-spared-some-shot-others-fifth-victim-dies

(Montana) **EPA pushes tough asbestos standard for Mont. town.** A proposed standard for federal cleanup of asbestos contamination in a Montana town concludes that even a tiny amount of the material can lead to lung problems — a benchmark far more rigorous than any in the past, and one the industry says could force expensive and unnecessary cleanups across the country. The U.S. Environmental Protection Agency's (EPA) new proposal for Libby, Montana, where asbestos dust has killed hundreds of people, would be 5,000 times stricter than the standard used in past cleanups addressing airborne asbestos. W.R. Grace & Co., the Maryland chemical company blamed for pollution from its vermiculite mine that operated for decades, argued sites across the country could be subjected to costly cleanups. The ongoing Superfund cleanup in Libby has cost at least $447 million since 1999 and is expected to last several more years. Experts said the EPA proposal is a move long sought by advocates and fiercely resisted by the industry. However, the Government Accountability Office has said the cleanup standard could affect some of the 200-plus industrial sites in 40 States that also received asbestos-tainted vermiculite from Grace's Montana mine. Federal agencies have also questioned the plan. They said the low threshold falls below even background asbestos levels seen in parts of the country. The EPA is to make a final decision on the standard for Libby sometime in 2013. Source: http://www.wistv.com/story/19659185/epa-pushes-tough-asbestos-standard-for-mont-town

National

Unexploded bombs lurk in U.S. offshore oil patch: Experts. Millions of pounds of unexploded bombs dumped in the Gulf of Mexico by the U.S. government after World War II pose a significant risk to offshore drilling, according to Texas oceanographers, Reuters reported September 28. The United States, along with other governments, dumped munitions and chemical weapons in oceans from 1946 until the practice was banned in the 1970s by U.S. law and international treaty, said a Texas A&M University professor of oceanography. As technological advances allow oil companies to push deeper into the waters of the Gulf of Mexico, these forgotten hazards pose a threat as the industry picks up the pace of drilling after BP Plc's deadly Macondo well blowout in 2010. Unexploded ordnance has been found in the offshore zone known as Mississippi Canyon where the Macondo well was drilled. The Bureau of Ocean Energy Management will auction 38 million acres of oil and gas leases in the central gulf in March. The U.S. government designated disposal areas for unexploded ordnance off the Atlantic and Pacific coasts, as well as in the Gulf of Mexico. However, nearly 70 years after the areas were created, no one knows exactly how much was dumped, or where the weapons are, or whether they present a danger to humans or marine life. In 2011, BP shut its Key Forties crude pipeline in the North Seas for 5 days while it removed a 13-foot unexploded German mine found resting next to the pipeline that transports up to 40 percent of the United Kingdom's oil product. Source: http://news.yahoo.com/unexploded-bombs-lurk-u-offshore-oil-patch-experts-173754705.html

INTERNATIONAL

3 countries join U.S. security alert in Philippines. Britain, Australia, and Canada have joined the United States in warning their citizens of a security threat in the Philippines, particularly in the capital, Manila. September 28, the U.S. Embassy in Manila said —reliable security forces detected a threat specifically in suburban Pasay City where it maintains a residential facility and a Veterans Affairs office. It urged U.S. citizens to avoid gatherings that may be regarded as —American events. The metropolitan Manila police chief said September 29 that he had ordered heightened security for embassies with increased patrols by uniformed and plainclothes officers. Such measures were put in place after attacks that killed the American ambassador in Libya. Source: http://www.usatoday.com/story/news/world/2012/09/29/us-security-alert-philippines/1602427/

Attack on U.S. Consulate in Libya determined to be terrorism tied to al-Qaeda. U.S. intelligence agencies have determined that the attack on the U.S. mission in Libya involved a small number of militants with ties to al-Qa'ida in North Africa but see no indication that the terrorist group directed the assault, U.S. officials said September 27. The determination reflects an emerging consensus among analysts at the CIA and other agencies that has contributed to a shift among senior Presidential administration officials toward describing the siege of U.S. facilities in Benghazi as a terrorist attack. U.S. intelligence officials said the composition of the militant forces involved in the assault has become clearer and that analysts now think two or three fighters affiliated with al-Qa'ida in the Islamic Maghreb (AQIM) were involved. U.S. officials said a lesser-known Islamist group, Ansar al-Sharia, played a much larger role in sending fighters and providing weapons for the attack, which killed the U.S. Ambassador and three other Americans. The intelligence picture assembled so far indicates militants had been preparing an assault on the U.S. compound in Benghazi for weeks but were so disorganized that, after the battle started, they had to send fighters to retrieve heavier weapons. U.S. intelligence officials said they think the attack was not timed to coincide with the September 11, 2001, anniversary. Instead, the officials said, the assault was set in motion after protesters scaled the walls of the U.S. Embassy in Cairo as part of a protest of an amateur anti-Islamic YouTube video. The State Department said September 27 that it was pulling more American staff from the U.S. Embassy in Tripoli out of concern for their safety. A State Department official described the reduction as temporary and said the embassy was not being closed. Source: http://www.washingtonpost.com/world/national-security/attack-on-us-consulate-in-libya-determined-to-be-terrorism-tied-to-al-qaeda/2012/09/27/8a298f98-08d8-11e2-a10c-fa5a255a9258_story.html

BANKING AND FINANCE INDUSTRY

Persistent flaws in PayPal allow cybercriminals to hijack user sessions and more. Multiple Web vulnerabilities have been identified by Vulnerability Lab researchers on the official PayPal Web site, Softpedia reported October 2. The high-severity security holes could have been exploited by a remote attacker against Pro, seller, or regular customer accounts. —A persistent input validation vulnerability is detected in the official Paypal ecommerce website content

management system (Customer/Pro/Seller). The bugs allow remote attackers to implement/inject malicious script code on the application side (persistent) of the paypal web service, the experts explained. —The vulnerability is located in the company profile input fields with the bound vulnerable address_id, details (mail) & companyname parameters. The bug affects the important user profile listing, the address listings & security notification (mail), they added. A similar vulnerability also affects the mail security notification module. If exploited successfully, the flaws could have allowed a cybercriminal to hijack user sessions, steal accounts via persistent Web attacks, and manipulate context in the affected modules. According to the experts, the payment processor was notified of the issues in July, but the security holes were addressed only in mid-September. Source: http://news.softpedia.com/news/Persistent-Flaws-in-PayPal-Allow-Cybercriminals-to-Hijack-User-Sessions-and-More-296107.shtml

DSL modem hack used to infect millions with banking fraud malware. Millions of Internet users in Brazil fell victim to a sustained attack that exploited vulnerabilities in DSL modems, forcing people visiting sites such as Google or Facebook to reach imposter sites that installed malicious software and stole online banking credentials, a Kaspersky security researcher said. The attack, described the week of September 24 during a presentation at the Virus Bulletin conference in Dallas, infected more than 4.5 million DSL modems, said the researcher, citing statistics provided by Brazil's Computer Emergency Response Team. The cross-site request forgery (CSRF) vulnerability allowed attackers to use a simple script to steal passwords required to remotely log in to and control the devices. The attackers then configured the modems to use malicious domain name system servers that caused users trying to visit popular Web sites to instead connect to booby-trapped imposter sites. Source: http://arstechnica.com/security/2012/10/dsl-modem-hack-infects-millions-with-malware/

Bank attackers more sophisticated than typical hacktivists, expert says. The hackers who said they were behind cyberattacks that disrupted the online operations of several U.S. banks the week of September 24 had technical firepower that went beyond the typical hacktivist, said one security expert. Experts debated the methods used in cyber-assaults on Wells Fargo, U.S. Bank, and PNC Bank, each struck on separate days, CSO Online reported September 28. The senior security evangelist at Akamai said the banks' Web servers were hit by as much as 65 gigabits of traffic per second, roughly as much as 60 times greater than the typical denial of service attack launched by hactivists. Also, the attackers used a single toolkit in building the programs that sent mostly junk data over the Internet to the banks' servers, he said. Hactivists typically use multiple toolkits running programs spread across compromised computers and systems of sympathizers. The attack traffic Akamai confronted was —fairly uniform, he said. —This does not happen with a hacktivist mob. A security researcher for FireEye who monitored the attack traffic has said he believes it was generated on hundreds of thousands of computers, many of which were likely owned by sympathizers of the attackers recruited through Web sites and social networks. He stuck by his people-powered theory, but agreed the attackers could have used a combination of servers and personal computers, some compromised and some belonging to sympathizers. Source: http://www.csoonline.com/article/717603/bank-attackers-more-sophisticated-than-typical-hacktivists-expert-says

American Express to refund $85 million to credit card customers. American Express Co. agreed to refund $85 million to 250,000 customers and pay $27.5 million in civil penalties after federal and State regulators found numerous violations of consumer protection laws. Among the alleged infractions were misleading some people who signed up for the company's Blue Sky credit card program into believing they would get a $300 payment they never received, charging improper late payments, and deceiving customers about the benefits of paying off old debts, the regulators said. The agency was among several regulators that conducted the investigation, which involved three American Express subsidiaries — American Express Centurion Bank, American Express Travel Related Services Co., and American Express Bank. Source: http://www.latimes.com/business/money/la-fi-mo-american-express-refund-fine-credit-card-20121001,0,238756.story

Fake Visa/Mastercard 'Security incident' notifications doing rounds. Bogus emails purportedly sent by the Visa/Mastercard —Identity Theft Department are targeting the cards' users by trying to convince them that a —security incident has put their online banking and credit card credentials at risk, Help Net Security reported September 27. Unfortunately for those users who click a link included in the emails, the destination page is a phishing page. —Although the fake form is not hosted on a secure (https) site as all genuine online financial transactions would be, the scammers have made an attempt to make the process seem more authentic by providing a typical image based security code field, Hoax-Slayer reported. —Users who enter the requested details will then be taken to further fake pages that request more financial and personal details. All information submitted on the bogus form will be sent to online criminals and used to make fraudulent transactions in the victim's name. Source: http://www.net-security.org/secworld.php?id=13679

BofA reaches $2.43 billion deal with investors over Merrill. Bank of America Corp. agreed to a $2.43 billion settlement with investors who suffered losses during its acquisition of Merrill Lynch & Co., resolving one of the biggest legal battles to stem from the takeover, Bloomberg News reported September 28. Bank of America faced regulatory probes, investor lawsuits, and criticism from lawmakers after buying Merrill in January 2009 for $18.5 billion without warning shareholders about spiraling losses at the brokerage before they voted to approve the deal. Under the settlement, Bank of America promised to overhaul corporate-governance policies. Shareholders sued in 2009 claiming Bank of America failed to disclose information about bonuses to Merrill employees and about the firm's financial losses in the fourth quarter of 2008. Source: http://www.bloomberg.com/news/2012-09-28/bofa-reaches-2-43-billion-deal-with-investors-over-merrill-1-.html

Chemical and Hazardous Materials Sector

Authorities in U.S. drill responses to 'dirty bomb' strikes. The United States the week of September 24 wrapped up a group of exercises in which national, State, and jurisdictional authorities weighed potential reactions to a hypothetical crisis involving multiple radiological —dirty bombs, the National Nuclear Security Administration (NNSA) announced. The last —Amber Waves 2012 drill enabled government personnel to address matters concerning the

assumption of administrative powers held by the interagency Federal Radiological Monitoring and Assessment Center during mitigation activities following a radiological strike, according to an NNSA press release. The Environmental Protection Agency's possible oversight of regions affected by harmful materials was another focus at the gathering. Kansas and Missouri hosted the Amber Waves 2012 events, which considered a potential attack incorporating synchronized dirty-bomb strikes in Leavenworth County, Kansas, and Kansas City, Missouri. Source: http://www.nti.org/gsn/article/us-authorities-drill-dirty-bomb-strikes/

(Arizona) **Man with fake ID arrested at Arizona nuclear plant.** Authorities said an illegal immigrant working for a construction company was arrested for trying to enter the grounds of the Palo Verde Nuclear Generating Station in Wintersburg, Arizona, with fake identification, the Associated Press reported September 26. Maricopa County sheriff's officials said the man was being held on suspicion of using false identification and criminal trespass onto a commercial nuclear generating station. Security personnel at the plant said the man showed an Arizona driver's license that appeared to be fraudulent. According to deputies, the man was interviewed at the scene and he was said to have admitted to using a fake ID and being in the country illegally. Authorities were investigating the construction company that hired him. Source: http://ktar.com/22/1577967/Man-with-fake-ID-arrested-at-Palo-Verde-plant

Commercial Facilities

Nothing Significant to Report

Communications Sector

Nothing Significant to Report

Critical Manufacturing

GM to recall about 41,000 cars over fuel leak problem. Reuters reported October 1 that General Motors Co (GM) is recalling about 41,000 Chevrolet, Pontiac, and Saturn cars in the United States because of concerns that a defective plastic part might cause a fuel leak, according to the National Highway Traffic Safety Administration. Potentially, 40,859 vehicles sold in Arkansas, Arizona, California, Florida, Nevada, Oklahoma, or Texas could be affected in the recall. As a remedial measure GM will notify owners, and dealers will replace the fuel pump module. Source: http://whtc.com/news/articles/2012/oct/01/gm-to-recall-about-41000-cars-over-fuel-leak-problem/

Honda expands North American recall to include over 600,000 Accords. Honda Motor Co is expanding a recall in North America to include more than 600,000 Accord mid-size sedans to address a potential power steering fluid leak problem that could cause a fire under the hood, Reuters reported October 1. Honda is recalling 573,147 Accords in the United States equipped with V6 engines from model years 2003 through 2007, according to documents filed with the U.S. National Highway Traffic Safety Administration. In Canada, 30,058 cars are also being

recalled, a company spokesman said. The power steering hose in the cars may deteriorate prematurely due to high temperatures, resulting in cracks and leaks that could cause a loss of power steering assistance or smoke and possibly a fire. No crashes or injuries have been reported related to the issue, but one engine fire was reported. The updated power steering hose necessary for the affected Accords will not be available until early 2013. If owners feel their cars exhibit symptoms related to a power steering hose leak, they should go to a dealer for an interim repair, Honda said. Source: http://whtc.com/news/articles/2012/oct/01/honda-expands-north-american-recall-to-include-over-600000-accords/

Defense/ Industry Base Sector

Russian agent sent advanced US military tech home: Feds. A Russian agent was arrested for allegedly using a Texas-based front company to send sensitive American technology to the Russian military and intelligence agencies, the Department of Justice said October 3. According to federal officials, the man was at the center of a Russian —military procurement ring that for years employed complex schemes to trick U.S. customs agents into believing his company was shipping harmless goods — like traffic light parts — to Russia, rather than advanced microelectronics that could be used in military applications including radar and surveillance systems, weapons guidance systems, or detonation triggers. The ring also allegedly provided microchips to a specialized electronics laboratory run by the FSB, Russia's intelligence agency and successor to the KGB. In addition to the agent, 10 other suspects working in the United States and in Russia were indicted for their alleged role in the scheme. The ploy was apparently so significant that U.S. officials said in court documents the front company's fluctuating revenue bore a —striking similarity to fluctuations in Russian defense spending over the last several years. Source: http://abcnews.go.com/Blotter/russian-agent-advanced-us-military-tech-home-feds/story?id=17385118#.UGxwP65T-Hs

Cyber era brings new kinds of supply-chain threats. Problems in the Defense Department's supply chain are not a new issue, however, the prevalence of digital systems brings a newer kind of threat: one that can be tiny in size but huge in potential impact. It is the risk of electronic components that have been altered to digitally infiltrate U.S. defense systems. The deputy assistant secretary of defense for manufacturing and industrial base policy admitted that Pentagon officials have seen cases of chips with —built-in back doors that could allow system access for espionage or data theft. Source: http://fcw.com/articles/2012/09/27/dod-supply-chain-cyber-era-problems.aspx

Chinese man charged in NYC carbon fiber sting. A Chinese national was charged September 26 in U.S. court with trying to broker an illegal deal for large quantities of carbon fiber, a restricted high-tech material used for military purposes. Prosecutors refused to say where and when he was arrested. The defendant made an appearance September 26 in federal court in Brooklyn, New York, on charges he sought the material for a fighter jet in China. A magistrate jailed him without bail. The defense attorney said his client lives in Quanzhou and works for a company that uses carbon fiber in the manufacturing of sports equipment. Authorities say higher-grade carbon fiber is a key component in aerospace and nuclear engineering. That has raised fears

that the material could pose a risk if it falls into the hands of military foes or terrorists, and made it the subject of tight Department of Commerce regulations. A criminal complaint accuses the Chinese national of contacting two Taiwanese accomplices, who already were under investigation in 2012, about buying specialized carbon fiber without an export license. —When I place the order, I place 1 to 2 tons, the Chinese national allegedly told one of the cohorts in a conversation intercepted in July. The complaint says 1 ton costs about $2 million. An undercover U.S. agent posing as a seller of carbon fiber later emailed the Chinese national, inviting him to the United States to meet about a possible deal. August 10, the Chinese national told the agent he was the middleman for a customer that —needed a sample of the carbon fiber because it would be used for the test flight of a _fighter plane' on Oct. 5, 2012, the complaint says. Source: http://www.businessweek.com/ap/2012-09-27/chinese-man-charged-in-nyc-carbon-fiber-sting

Emergency Services

(Arizona) **Border Patrol agent shot, killed on patrol in Ariz.** A U.S. Border Patrol agent was killed and another wounded in a shooting October 2 in Arizona near the U.S.-Mexico line, according to the Border Patrol. The agents were shot while patrolling on horseback in Naco, Arizona, October 2, the Border Patrol said in a statement. The agents who were shot were on patrol with a third agent, who was not harmed, according to the president of the National Border Patrol Council, a union representing about 17,000 border patrol agents. The shooting occurred after an alarm was triggered on one of the many sensors along the border and the three agents went to investigate, said a Cochise County Sheriff's spokeswoman. Authorities have not identified any suspects, she said. It is not known whether the agents returned fire. The wounded agent was airlifted to a hospital after being shot in the ankle and buttocks, the Border Patrol said. That agent was in surgery and expected to recover said the union president. Source: http://www.myrtlebeachonline.com/2012/10/02/3092994/homeland-security-says-border.html

(North Carolina) **KKK leader in NC convicted on weapons charges.** A Ku Klux Klan leader from North Carolina was convicted on weapons and explosive charges related to a plot to blow up the Johnston County sheriff, the Associated Press reported September 28. A jury convicted the leader on six felony counts the week of September 25, including conspiracy, possession of stolen guns, and receipt of explosives with intent to kill. Prosecutors said the Klansman wanted to kill the sheriff, whom he blamed for the failure of his nightclub. He also blamed the sheriff for the Klan not being permitted to march in Benson's annual Mule Days parade. According to trial testimony, the Klan leader acquired powerful explosives and planned to boat down the Neuse River at night to plant a bomb at the sheriff's office without being seen. Source: http://www.fresnobee.com/2012/09/28/3009655/kkk-leader-in-nc-convicted-on.html

Energy

Nothing Significant to Report

Food and Agriculture

Report: Some dietary supplements illegally labeled. Dozens of weight loss and immune system supplements on the market are illegally labeled and lack the recommended scientific evidence to back up their purported health claims, government investigators warned in a new review of the $20 billion supplement industry. The report, released October 3 by the Department of Health and Human Services' inspector general, found that 20 percent of the 127 weight loss and immune-boosting supplements investigators purchased online and in retail stores across the country carried labels that made illegal claims to cure or treat disease. Some products went so far as to state the supplements could cure or prevent diabetes or cancer, or that they could help people with HIV or AIDS, which is strictly prohibited under federal law. Federal rules do not require the Food & Drug Administration (FDA) to review supplement companies' scientific evidence for most of their products' purported health benefits before they hit the market. In response, the food safety agency said it would consider asking Congress for more oversight powers to review supplement companies' evidence proving their products' purported health benefits. FDA agreed that the agency should expand surveillance of the market to detect spurious claims that supplements can cure or treat specific diseases. Investigators also found that 7 percent of the weight loss and immune support supplements they surveyed lacked the required disclaimer stating that FDA had not reviewed whether the statement on the label was truthful. Source: http://www.thecalifornian.com/article/20121003/NEWS06/310030025/Report-Some-dietary-supplements-illegally-labeled

Canadian beef recall grows, again. October 2, Food Safety News reported the thirteenth expansion of the XL Foods, Inc. recall. Alberta, Canada-based XL Foods, Inc. is voluntarily recalling 260 more varieties of beef, announced the Canadian Food Inspection Agency in a health alert October 1. These newly recalled meats have been added to hundreds of other beef products recalled by the company in the past 2 weeks. Some beef products listed in this latest recall — including rump roast, soup bones, and tenderized hip steak among others — were not listed in previous recall updates that have mainly included ground beef and various whole and tenderized cuts. Products affected by this update were manufactured on the same dates as XL's previously recalled ground beef products — August 24, 27, 28, 29, and September 5. Affected products were sold in retail stores across the United States, including Dominion, Extra Foods, Real Atlantic, Save Easy, ValuFoods, Valu-mart, VillageMart, and Zehrs, among others. The XL Foods recall has so far affected U.S. retailers in 41 States, and has rendered over 1,100 beef products unsafe. Source: http://www.foodsafetynews.com/2012/10/canadian-beef-recall-grows-again/#.UGru7pGvMcs

General Mills issues voluntary class one recall of one day's production of Almond Nature Valley Sweet & Salty Nut Granola Bars. September 26, the U.S. Food and Drug Administration reported that General Mills voluntarily recalled a single day's production of Almond Nature Valley Sweet & Salty Nut Granola Bars because of a labeling issue. Product produced on this date may have been packaged incorrectly, and may contain allergens not listed on the box's ingredient label, specifically peanuts. A production error resulted in a limited number of

properly labeled, individually wrapped Peanut Nature Valley Sweet & Salty Nut Granola Bar packages being inserted into six-count boxes labeled as Almond Nature Valley Sweet & Salty Nut Granola Bars. The recalled boxes have a better-if-used-by date of February 26, 2013. Source: http://www.fda.gov/Safety/Recalls/ucm321340.htm

FSIS expands Public Health Alert for imported Canadian beef from XL Foods. September 28, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) expanded the Public Health Alert for XL Foods to include all beef and beef products produced August 24, 27, 28, 29 and September 5. Products subject to the recall include, but are not limited to, steaks, roasts, mechanically tenderized steaks and roasts, and ground beef. The Canadian Food Inspection Agency notified FSIS that XL Foods expanded the recall. Source: http://www.fsis.usda.gov/News_&_Events/NR_092812_01/index.asp

Government Sector (including Schools and Universities)

U.S. Cyber Command officer says China is targeting Pentagon computers. September 27, the U.S. Cyber Command's top intelligence officer accused China of persistent efforts to pierce Defense Department computer networks. He said a proposal was moving forward to boost the cyber command in the U.S. military hierarchy. —Their level of effort against the Department of Defense is constant while alleged Chinese attempts to steal corporate trade secrets has been growing, the command's director of intelligence told Reuters after remarks to a forum on the history of cyber threats. The Office of the National Counterintelligence Executive, a U.S. intelligence arm, said in a landmark report a year ago that —Chinese actors are the world's most persistent perpetrators of economic espionage. —It's continuing apace, the top officer said. —In fact, I'd say it's still accelerating. He accused China of trying to exfiltrate Defense Department secrets. Asked whether any classified U.S. networks had been successfully penetrated — something not publicly known to have occurred — he replied: —I can't really get into that. A spokesman for the Chinese embassy did not immediately respond to a request for comment. In the past Chinese officials have denied such accusations. Source: http://www.huffingtonpost.com/2012/09/27/samuel-cox-us-cyber-command-china_n_1921465.html?utm_hp_ref=technology

Information Technology and Telecommunications

Google warns of new state-sponsored cyberattack targets. Beginning October 2, tens of thousands more Google users will begin to see a message at the top of their Gmail inbox, Google home page, or Chrome browser that state-sponsored attackers may be attempting to compromise their account or computer. The company said that since it started alerting users to malicious — probably state-sponsored — activity on their computers in June, it has picked up thousands of more instances of cyberattacks than it anticipated. A manager on Google's information security team said that since Google started to alert users to state-sponsored attacks 3 months ago, it gathered new intelligence about attack methods and the groups

deploying them. He said the company was using that information to warn —tens of thousands of new users that they may have been targets. Source: http://bits.blogs.nytimes.com/2012/10/02/google-warns-new-state-sponsored-cyberattack-targets/

Zombie-animating malnets increase 300% in just 6 months. Cyber criminals are bolstering the infrastructure behind the delivery of botnets, a move that is leading toward more potent and numerous threats, say researchers. Botnet infections are commonly spread though compromised Web sites seeded with malicious scripts and promoted via black hat SEO tactics such as link farms. These malware networks, or malnets, pose a growing threat, according to a new study by Web security firm Blue Coat. Malnets largely deal in mass-market malware, and, as such, are different from advanced persistent threats (APTs) associated with cyber-espionage attacks targeting large corporations and Western governments. Attacks will be updated and changed, but the underlying infrastructure used to lure in users and deliver these attacks is reused. The ease with which cyber criminals can launch attacks using malnets creates a vicious cycle, a process by which individuals are lured to malware, infected, and then used to infect others. Source: http://www.theregister.co.uk/2012/10/03/malnets/

Twitter authentication flaw allows hackers to hijack user accounts. Cyber criminals can steal Twitter accounts by leveraging a flaw in the social network's authentication system. In a recent case, a hacker utilized software that repeatedly tests common passwords against the account. This type of brute force attack is possible because Twitter only limits the log-in attempts if they come from the same IP address. Most Web sites implemented a system that prevents potential criminals from hijacking accounts by trying out random passwords. However, since Twitter only prevents multiple log-in attempts from the same computer, attackers can try out as many passwords as they want as long as they change their IP address. Source: http://news.softpedia.com/news/Twitter-Authentication-Flaw-Allows-Hackers-to-Hijack-User-Accounts-296206.shtml

Prolexic: 'itsoknoproblembro' DDoS attacks are highly sophisticated. Experts from Prolexic Technologies claim a new type of distributed denial-of-service (DDoS) attack has not only increased in size, but also reached a new level of sophistication. DDoS attacks have recently caused a lot of problems for organizations; in September, the sites of several financial institutions were disrupted as a result of such operations. Prolexic found that many of the recent attacks against their customers relied on the itsoknoproblembro DDoS toolkit. By combining the toolkit's capabilities with other sophisticated methods, the cyber criminals have been able to launch attacks that are difficult to mitigate even for specialized firms. Prolexic recorded massive sustained floods, some of which peaked at 70 Gbps and over 30 million pps. Itsoknoproblembro includes a number of application layer and infrastructure attack vectors, such as UDP and SSL encrypted attack types, SYN floods, and ICMP. The botnet that powers these attacks contains a large number of legitimate IP addresses. This allows the attack to bypass the anti-spoofing mechanisms deployed by companies. Source: http://news.softpedia.com/news/Prolexic-quot-itsoknoproblembro-quot-DDOS-Attacks-Are-Highly-Sophisticated-296180.shtml

Phishing attacks cast wider nets in businesses. Phishing attacks are moving from targeting a few key employees in businesses to much wider groups of employees, according to corporate security awareness training company PhishMe. —Once they are in, attackers are using what they learn about the environment to attack bigger groups, said the company's vice-president of product management and services. Some organizations are seeing phishing campaigns targeted at up to 250 employees at a time, but using slightly different fake emails to avoid detections systems, he told Computer Weekly. Phishing attacks are also moving away from using attachments because of greater awareness among corporate users about the potential dangers of email attachments. Instead, they are using emails about topical or local events likely to be of general interest to just about anyone in the organization. Source: http://www.computerweekly.com/news/2240164139/Phishing-attacks-cast-wider-nets-in-businesses

Brute force attack can break PINs of Cisco CallManager accounts, researcher finds. While performing a review of Cisco's Unified Communications Manager (CallManager), a software-based call-processing system, a security researcher found a way to break the PINs of registered accounts by performing a brute force attack. —When looking at the phone handset configuration, some URLs are set to allow the handset to retrieve Personal Address Book details or access the Fast Dials. That caught my attention and I immediately pointed my web proxy to those URLs, forgetting about the handset interface, the expert explained. The researcher noticed the handset itself is actually performing simple GET HTTP requests to the CallManager to initiate the log-in sequence. The response contains a —sid token which is needed to perform the brute force attack. Since it is not possible to perform a userID enumeration, the attack is done with an application such as Burp. Source: http://news.softpedia.com/news/Brute-Force-Attack-Can-Break-PIN-of-Cisco-CallManager-Researcher-Finds-295989.shtml

Analysis shows some URL shorteners often point to untrusted Websites. In an analysis of 1.7 billion shortened URLs, researchers at Web of Trust found that 8.7 percent of TinyURLs and 5 percent of Bit.ly URLs led to sites that received poor ratings for —trustworthiness and —child protection. —Certainly the URL shortening services do not intend to point people to malicious websites, said Web of Trust's CEO, —but perhaps they can do more to proactively protect their services from being exploited. Web of Trust goes on to point out that many countries' TLDs through which link shortening services route traffic are loosely regulated and return suspicious ratings for as many as 90 percent of the Web sites under their top level domains. Source: http://threatpost.com/en_us/blogs/analysis-shows-some-url-shorteners-often-point-malicious-websites-092712

Building Android malware is trivial with available tools. Because of readily available tools that enable even a novice developer to create malicious mobile applications, users should be cautious when downloading and installing mobile apps, especially from non-official App Stores. Developing Android malware to harvest information is a —trivial task and possible using readily available tools, a security architect and director at Kindsight Security Labs told

SecurityWeek. He demonstrated how to inject snippets of code into a legitimate Android application that infected a mobile device with malware. The malware, when executed, connected with a remote command-and-control center and transmitted data from the device. Source: http://www.securityweek.com/building-android-malware-trivial-available-tools

Adobe code signing infrastructure hacked by 'sophisticated threat actors'. September 27, Adobe warned that an internal server with access to its digital certificate code signing infrastructure was hacked by —sophisticated threat actors engaged in —highly targeted attacks. The compromise, which dates back to early July, led to the creation of at least two malicious files that were digitally signed using a valid Adobe certificate, according to Adobe's security chief. Although only two files were signed, the hack effectively gave the attackers the ability to create malware masquerading as legitimate Adobe software and signals a raising of the stakes in the world of Advanced Persistent Threats (APTs). According to the security chief, one of the two digitally signed malware files is a utility that extracts password hashes from the Windows operating system. Source: http://www.zdnet.com/adobe-code-signing-infrastructure-hacked-by-sophisticated-threat-actors-7000004925/

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

Fungal meningitis suspected in four deaths, 26 cases as outbreak grows. Four people have died and 22 more were made sick by meningitis linked to a rare fungal infection blamed on contaminated steroids, health officials said October 3. They are —almost certain more will be identified before it is over. The 26 cases include 18 people in Tennessee, 1 in North Carolina, 2 in Florida, 3 in Virginia, and 2 in Maryland, the U.S. Centers for Disease Control and Prevention reported. Two of the deaths were in Tennessee, one in Virginia, and one in Maryland. The chief suspect is contaminated vials of a pain treatment injected directly into the spine. The drug, called methylprednisolone acetate, was made by a compounding pharmacy — one that makes drugs to order. The suspected batches were made without any preservatives. Several of the patients are seriously ill, said the Tennessee Department of Health commissioner. Two clinics have closed voluntarily and a third is no longer giving the injections. Source: http://vitals.nbcnews.com/_news/2012/10/03/14203956-fungal-meningitis-suspected-in-four-deaths-26-cases-as-outbreak-grows?lite

FDA: Most online pharmacies fraudulent. The Food and Drug Administration was warning U.S. consumers that the vast majority of Internet pharmacies are fraudulent and likely selling counterfeit drugs that could harm them. The agency September 28 launched a national

campaign, called BeSafeRx, to alert the public to the danger amid evidence that more people were shopping for their medicine online. Research by the National Association of Boards of Pharmacy, which represents State pharmacy boards, found that of thousands of online pharmacies it reviewed, only about 3 percent follow State and federal laws. The campaign comes after some high-profile cases of counterfeit drugs reaching American patients earlier in 2012. Source: http://www.telegram.com/article/20120928/NEWS/120929530/-1/NEWS06#.UGm0Ca6Wimh

(Indiana) **Homeland security officials investigate substance found at Riley Hospital for Children.** Seven people became ill after a strong odor overtook the emergency room at Riley Hospital for Children September 27 in Indianapolis. The emergency room was evacuated. Indianapolis Homeland Security officials awaited lab results September 28. Four of the seven affected adults were treated and released, said the hospital CEO. He said the remaining three patients were receiving treatment at another hospital. Indianapolis Fire Department crews also responded. Indianapolis Metro Police Department officers said they were not ruling out criminal activity. Operations within Riley's ER returned to normal September 28. Source: http://www.theindychannel.com/news/local-news/homeland-security-officials-investigate-substance-found-at-riley-hospital-for-children

Transportation

Report: Amtrak employees failing drug, alcohol tests at alarming rate. A report blasts Amtrak, the nation's largest passenger rail carrier, for dangerously overlooking drug and alcohol use by its employees, CNN reported October 1. The report released September 27, an internal audit by Amtrak's Office of Inspector General, says drug and alcohol use by employees has steadily risen since 2006. The majority of employees who failed drug tests were reported to have tested positive for cocaine and marijuana, according to the report. Amtrak's employees failed drug and alcohol tests at a staggering 51 percent higher rate than the rail industry average, the report says. Amtrak officials estimated that they have spent $1.5 million to screen employees in 2012 alone, but employees have exceeded industry averages failing drug tests in each of the past 5 years. Federal regulations requiring railroad companies to implement drug and alcohol testing were put in place after a deadly 1987 Amtrak collision with a freight train in Chase, Maryland. In that accident, investigators concluded that a Conrail freight train engineer was under the influence of marijuana and ran three signals before colliding with the passenger train, killing 16. The report suggested many ways Amtrak could prevent employees from showing up to work drunk and on illegal drugs. The recommendations include increasing the frequency of drug and alcohol testing, reviewing results and comparing them to industry averages, demonstrating that drug and alcohol control is a priority for Amtrak senior management, improving the physical observation of employees, and increased training of supervisors. Source: http://www.cnn.com/2012/09/28/travel/amtrak-drug-alcohol-tests/index.html

(California) **BART to adopt earthquake early warning system.** Thanks to assistance from the Berkeley Seismological Laboratory, the San Francisco Bay Area Rapid Transit (BART) system can now automatically brake trains when earthquakes threaten to rattle the Bay Area, allowing

perhaps tens of seconds to a minute for trains to slow down before the ground starts to shake, Homeland Security News Wire reported September 28. Instituted in August, the earthquake early warning system was created with the help of University of California (UC), Berkeley, seismologists who hooked BART into data flowing from the more than 200 stations throughout Northern California of the California Integrated Seismic Network. —The earthquake early warning system will enable BART to stop trains before earthquake shaking starts, and thereby prevent derailment and save passengers from potential injuries, said the BART board president. He was joined by a UC Berkeley seismologist who discussed plans for a broader early warning system along the Pacific Coast that would rival Japan's well-known earthquake early warning system, which not only slows trains but alerts schools and can even automatically shut valves at industrial sites. Source: http://www.homelandsecuritynewswire.com/dr20120928-bart-to-adopt-earthquake-early-warning-system

Water and Dams

(Ohio) **Thieves cause $100K in damage to storm system.** Thieves who stole a vital piece of the Dayton, Ohio storm water control system and caused $100,000 in damage have set off a thorough check by city workers to determine whether other thefts went undetected, the Dayton Daily News reported September 27. Investigators were not sure when thieves made off with a 700-pound bronze shaft that was 15 feet long and used to control a 10,000-pound flood gate along the Mad River. The theft was discovered the weekend of September 22. DHS was notified, police said. The gate and 115 others like it in the system were engineered to control street storm water runoff to the river. City workers checked all gate installations for other thefts, and the city put the word out to local scrap metal businesses to be on the lookout. The thieves built a special ladder to get into the mechanical workings of the control system inside an underground vault to steal more metal parts. Source: http://www.daytondailynews.com/news/news/metal-thieves-cause-100000-to-city-storm-water-con/nSNcH/

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