

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

Nothing Significant to Report

REGIONAL

(Minnesota) Confirmed norovirus outbreak in Mankato. The Minnesota Department of Health confirmed that an outbreak of norovirus occurred at the Verizon Wireless Center in Mankato, Minnesota the week of November 12. A Minnesota Department of Health spokesperson said it is likely that more than 50 people attending a Chamber of Commerce event November 13 and a veterans' event November 14 were sickened in the outbreak. Norovirus is spread through stool and can be transmitted through food or on surfaces. The agency was still investigating the cause of the outbreak. He said the facility has made some changes to avoid further possible transmission of the virus. November and December is typically when most norovirus cases in Minnesota occur. Source:

<http://minnesota.publicradio.org/display/web/2012/11/20/health/sickness-outbreak-in-mankato-may-be-a-virus/>

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Suicide blast hits near U.S. base in Kabul. Two Taliban suicide bombers struck near a U.S. base in Kabul November 21, killing two Afghan guards in the heart of a neighborhood filled with foreign forces and embassies. The attack came despite increased security ahead of a Muslim holy day that last year saw one of the capital's deadliest attacks. The bombers apparently meant to target the American base but were spotted by security guards as they approached on foot. The guards fired on the assailants, killing them, but not before one of the vests exploded, said the deputy provincial police chief. Two Afghan security guards were killed and five civilians were wounded in the morning explosion, he said. The blast reverberated around Kabul's Wazir Akbar Khan neighborhood. An alarm started going off at the nearby U.S. Embassy, warning staff to take cover. The Taliban claimed responsibility for the bombing in an email to reporters.

Source: <http://www.militarytimes.com/news/2012/11/ap-suicide-blast-hits-near-us-base-in-afghanistan-112112/>

BANKING AND FINANCE INDUSTRY

Fake Apple invoices in your inbox could lead to empty bank accounts. Fake Apple invoices are appearing in inboxes that contain a Blackhole exploit kit and a trojan that is designed to log users' keystrokes and ultimately compromise bank accounts, Silicon Republic reported November 23. The multi-pronged approach was discovered by a Sophos researcher who reported it in the Naked Security blog. The online criminals who circulated the fake invoices are

UNCLASSIFIED

UNCLASSIFIED

using a form of social engineering where users think they are being billed for an expensive product they never bought, in the researcher's case, he received an invoice telling him he ordered and paid for goods valued at \$699. If a user clicks on any of the links contained in the email they are taken to a page proclaiming to be the IRS telling them their browser is unsupported and offers a range of browser options. As the page is displayed, the user's computer gets infected with the Zeus/Zbot trojan. If the user clicks on any of the browser options, a file labeled update.exe is downloaded. If the user opens the file their computer is automatically infected with the trojan, which is designed to record keystrokes and ultimately give criminals the information they need to access the user's bank account online. Source: <http://www.siliconrepublic.com/strategy/item/30388-fake-apple-invoices-inyour/>

Shadow banking hits \$67 trillion globally: task force. The shadow banking system - blamed for aggravating the financial crisis - grew to a new high of \$67 trillion globally in 2011, a top regulatory group said, calling for tighter control of the sector. A report by the Financial Stability Board (FSB) November 18 appeared to confirm fears among policymakers that the so-called shadow banking system of non-bank intermediaries continues to harbor risks to the financial system. The FSB, a task force from the world's top 20 economies, also called for greater control of shadow banking, a corner of the financial universe made up of entities such as money market funds that has so far escaped the web of rules that is tightening around traditional banks. The European Commission is expected to propose E.U.-wide rules for shadow banking in 2013. The United States is already rolling out a framework of new rules for the \$2.5 trillion money market industry. The FSB said shadow banking around the world more than doubled to \$62 trillion in the 5 years to 2007, and had grown to \$67 trillion in 2011 - more than the total economic output of all the countries in the study. America had the largest shadow banking system, said the FSB, with assets of \$23 trillion in 2011, followed by the Euro area with \$22 trillion, and the United Kingdom at \$9 trillion. The U.S. share of the global shadow banking system has declined in recent years, the FSB said, while the shares of the United Kingdom and the euro area have increased. Source: <http://www.chicagotribune.com/business/sns-rt-us-shadow-banking-regulationbre8ai0sl-20121119,0,7490614.story>

The housing scam that's targeting vets and seniors. The housing market is bouncing back, and so are deceptive marketing practices. That has prompted the U.S. Consumer Financial Protection Bureau (CFPB) and the U.S. Federal Trade Commission to launch investigations into six mortgage lenders and brokers that allegedly target veterans and senior citizens with misleading advertising, Bloomberg News reported November 20. The regulators also sent warning letters to a dozen more companies, urging them to review their marketing materials and be sure they are not breaking federal law. The lenders appeared to be trying to dupe consumers into thinking loans were government-backed, according to the CFPB. Some of the ads sent to the elderly included a return address line that read "Government Loan Department," used a logo that resembled the seal of the U.S. Department of Housing and Urban Development, and displayed a Web URL bearing the initials of the Federal Housing Administration, the CFPB said. Veterans received ads that appeared to come from the U.S. Department of Veteran's Affairs (VA) and offered rates under a special "economic stimulus plan" said to be expiring soon, according to the CFPB. The ads began with the phrase, "The VA is

UNCLASSIFIED

UNCLASSIFIED

offering you,” and used logos similar to the VA’s. The ads also promised a “fixed” rate for a 30-year loan even though the fine print indicated that the rates were adjustable, according to the CFPB. Source: <http://www.businessweek.com/articles/2012-11-20/holly-petraeuss-crackdown-on-alleged-mortgage-swindlers>

Professional trojan targets SEPA transactions. Cyber-criminals are targeting the European SEPA payments network, according to a report from security specialist McAfee, The H reported November 21. Within the E.U., SEPA transactions are uncomplicated because they make no distinction between domestic and cross-border transactions. In this case, that also benefits the online crooks who usually transfer money from the victim’s account to foreign bank accounts. The report says the malware involved is part of “Operation High Roller” where criminals extracted large sums from business accounts. The malware acts in a remarkably similar manner to how Zeus and others work: after infection it inserts itself into the system’s browser and waits for a user to access their bank’s Web site. Once there, the pest adds its own JavaScript code, called Web Injects, to perform the fraudulent withdrawals. The malware takes its instructions from a command and control server which is, McAfee says, located in Moscow. The software is hard-coded to withdraw amounts ranging between 1,000 Euros to 100,000 Euros depending on the balance of the account. Source: <http://www.h-online.com/security/news/item/Professional-trojan-targets-SEPA-transactions-1754446.html>

EAST releases ATM fraud update; U.S. still attracts most fraud. The European ATM Security Team (EAST) published its third European Fraud Update for 2012, ATM Marketplace reported November 21. It reveals that the U.S. still ranks first for skimming fraud, and also finds that fraudsters are shifting their attention from markets where EMV is used to those where it is not — meaning that the U.S. is likely to retain its dubious distinction for some time. The update is based on crime reports from representatives of 18 countries in the single euro payments area (SEPA), as well as representatives of three non-SEPA countries. All but four countries reported continued skimming attacks at ATMs. In addition to ATMs, skimming was reported at unattended payment terminals at petrol stations, and at parking ticket machines, railway ticket machines, and point of sale (POS) terminals. Fraud losses continue to migrate away from EMV liability shift areas. The U.S. remains the top location for such losses, followed by Mexico, the Dominican Republic, and Brazil. Card issuers are continuing to take measures to block the use of payment cards outside of designated EMV liability shift areas. Eight countries now report the use of some form of geo-blocking. Fifteen countries reported cash-trapping incidents, but such attacks seem to be stabilizing or falling in most countries. Eight countries reported ram raids and ATM burglary — in many cases these were unsuccessful, but still caused significant collateral damage. Source: <http://www.atmmarketplace.com/article/204097/EAST-releases-ATM-fraud-update-US-still-attracts-most-fraud>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

UNCLASSIFIED

COMMERCIAL FACILITIES

(California) Three dead in murder-suicide at California senior center. Three people died November 20 in what appeared to be a double murder-suicide at a senior citizens' high-rise in Torrance, California, police said. A man in his 80s apparently shot two women before turning the gun on himself in the lobby of the Golden West Tower apartments, a police spokesman said. One of the women was an employee of the apartment complex, but victim identities were withheld until the next of kin was notified. Police were still investigating the man's motive, but residents and staff from the senior center told reporters that the man had been behaving erratically, and many of them were seeking to have him kicked out of the complex. A handgun was recovered at the scene. Police were trying to obtain surveillance camera recordings of the shooting, the spokesman said. According to the city of Torrance's Web site, Golden West Towers is a 180-unit, privately owned and operated facility. The low- and moderate-income housing is for seniors who can live independently. The incident was the latest in a string of murder-suicides at senior centers in southern California in recent years. Source: <http://www.ajc.com/ap/ap/california/3-killed-in-double-murder-suicide-at-senior-center/nTBx7/>

COMMUNICATIONS SECTOR

Nothing Significant to Report

CRITICAL MANUFACTURING

Toyota recalls 160,000 Tacoma pickups in U.S. and Canada. Toyota Motor Corp announced November 21 the recall of about 160,000 Tacoma mid-size pickup trucks from model years 2001 to 2004 in 20 coldweather U.S. States and in Canada because the spare tire could fall off. The spare tire in these Tacoma models is stored beneath the trucks' bed. When the trucks were made, the metal plate that keeps the spare tire in place was not coated with sufficient amounts of phosphate to retard rust, Toyota said. Two accidents have been reported to Toyota involving vehicles following a Tacoma truck. Over time and in limited cases, corrosion of the plate could cause it to break, causing the detachment of the spare tire. Letters will go to the owners of the recalled vehicles in December, and Toyota dealers will replace the spare tire assembly, if necessary. Source: <http://wkzo.com/news/articles/2012/nov/21/toyota-recalls-160000-tacomapickups-in-us-and-canada/>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

(Pennsylvania) Philadelphia Police Department joins Pinterest. The Philadelphia Police Department (PPD) is utilizing social media to catch criminals, by joining Pinterest, KYW 3

UNCLASSIFIED

Philadelphia reported November 19. The department's boards are full of mugshots, divided up by division. Police made the announcement they had joined the social media bigwig over Twitter, posting "PhillyPolice is now on #Pinterest. We have a board for your section of the city," with a link. In addition to mugshots, the PPD's Pinterest page also features boards for "Cops in the Community," "Safety and Prevention," and "Inside the PPD." Source: http://philadelphia.cbslocal.com/2012/11/19/philadelphia-police-department-joins-pinterest/?hpt=us_bn7

ENERGY

Nothing Significant to Report

FOOD AND AGRICULTURE

Whole Alternatives, LLC recalls Harris Teeter Dried Apricots and Dried Golden Raisins due to undeclared sulphur dioxide. Whole Alternatives, LLC ("Whole Alternatives") of Louisville, Kentucky, initiated a voluntary recall November 19 of Harris Teeter brand six ounce packages of dried apricots and Harris Teeter brand eight ounce packages of dried golden raisins because the products contain undeclared sulphur dioxide. The recalled dried apricots and dried golden raisins were distributed in Harris Teeter stores. The apricots are packaged in 6 ounce, clear plastic bags and raisins in 8 ounce, clear plastic bags and all lot numbers and code dates are affected. The recall was initiated after Whole Alternatives discovered the product was distributed in packages which did not declare sulphur dioxide as an ingredient on the label. Source: <http://www.fda.gov/Safety/Recalls/ucm329019.htm>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

White House issues insider threat guidance to agencies. The White House November 21 issued new minimum standards for agencies to guard against insider security threats such as those that led to a 2010 breach. In a memo, the U.S. President directed agencies to install programs to thwart internal threats, including espionage, violent acts against the government, and unauthorized disclosures of classified information and sensitive data stored on government computer networks and systems. According to the memo, minimum standards for a government wide insider threat program should include: The ability to gather, integrate, and centrally analyze and respond to key threat-related information, the ability to monitor employees' use of classified networks, insider threat awareness workforce training, and protections of civil liberties and privacy of all personnel. Source: <http://www.federaltimes.com/article/20121121/AGENCY04/311210002/White-Houseissues-insider-threat-guidance-agencies>

UNCLASSIFIED

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Exploitation of privileged access points: Common vector for high-profile attacks. A study performed by information security firm Cyber-Ark labs reveals that, in most of the recent high-profile cyberattacks, the common attack vector is the exploitation of privileged access points. These privileged access points usually consist of administrative or privileged accounts, application backdoors, and hardcoded or default passwords. In recent months, privileged access points have been utilized in the Flame attacks, and the ones against companies such as Saudi Aramco and Subway. The executive vice president Americas of Cyber-Ark Software explains that cybercriminals are well aware of the power and wide ranging access provided by these access points, which is the main reason why future attacks will also target them. Source: <http://news.softpedia.com/news/Exploitation-of-Privileged-Access-Points-Common-Attack-Vector-for-High-Profile-Attacks-308594.shtml>

Yahoo email-stealing exploit fetches \$700. A zero-day vulnerability in yahoo.com that lets attackers hijack Yahoo! email accounts and redirect users to malicious Web sites offers a fascinating glimpse into the underground market for large-scale exploits. The exploit, being sold for \$700 by an Egyptian hacker on an exclusive cybercrime forum, targets a “cross-site scripting” (XSS) weakness in yahoo.com that lets attackers steal cookies from Yahoo! Webmail users. Such a flaw would let attackers send or read email from the victim’s account. “I’m selling Yahoo stored xss that steal Yahoo emails cookies and works on ALL browsers,” wrote the vendor of this exploit, using the hacker handle ‘TheHell.’ “And you don’t need to bypass IE or Chrome xss filter as it do that itself because it’s stored xss.” Krebs On Security alerted Yahoo! to the vulnerability, and the company says it is responding to the issue. The director of security at Yahoo! said the challenge now is working out the exact yahoo.com URL that triggers the exploit. Source: <http://krebsonsecurity.com/2012/11/yahoo-email-stealing-exploit-fetches-700/>

Password-stealing malware Passteal distributed via file sharing sites. Experts warn that Passteal, the piece of malware that steals sensitive information stored in Web browsers by relying on password recovery tools, is being distributed through file sharing Web sites. Trend Micro researchers identified Passteal versions disguised as e-books, key generators, and even bundled with installer applications. While older variants relied on PasswordFox to gain access to sensitive browser data, a new version (TSPY_PASSTEAL.B) has been found to use WebBrowserPassView instead. This enables the attackers to steal information from Internet Explorer, Firefox, Chrome, and Safari. Source: <http://news.softpedia.com/news/Password-Stealing-Malware-Passteal-Distributed-Via-File-Sharing-Sites-308650.shtml>

HTTP Strict Transport Security becomes Internet Standard. The Internet Engineering Task Force (IETF) published RFC 6797, formally declaring the HTTP Strict Transport Security (HSTS) security mechanism for HTTPS as an Internet Standard. HSTS is designed to allow HTTP servers to ensure that any services offered can only be accessed via secure connections that are encrypted using mechanisms such as Transport Layer Security (TLS). From a client perspective, HSTS forces applications (User Agents) to only use encrypted connections when communicating with Web sites. The primary aim of HSTS is to counteract the attacks on SSL-encrypted Web

UNCLASSIFIED

sites that were described by a security researcher in 2009. The attacks take advantage of the fact that users do not generally use https:// to access a page but rather tend to visit the unencrypted URL and then trust that they will be redirected to the HTTPS version in due course. The attacks prevent this redirection without triggering alerts. Source: <http://www.h-online.com/security/news/item/HTTP-Strict-Transport-Security-becomes-Internet-Standard-1754549.html>

NATIONAL MONUMENTS AND ICONS

(California) Yosemite hantavirus outbreak has sickened 10, killed 3, CDC says. To date, 10 people have fallen ill — and 3 have died — in the hantavirus outbreak at California's Yosemite National Park's "signature" cabins in Curry Village, according to the U.S. Centers for Disease Control and Prevention (CDC), the Los Angeles Times reported November 21. At Yosemite, deer mice infected with the Sin Nombre strain of hantavirus took up residence in the insulation in the signature cabins. Nine of the 10 human hantavirus cases occurred in guests who had stayed in the cabins, researchers from State public health agencies, the National Park Service and the CDC said in a brief article issued November 21 in the CDC's Morbidity and Mortality Weekly Report. The researchers also reported that the 10 patients came from California, Pennsylvania, and West Virginia, and were between 12 and 56 years of age. Nine had typical symptoms of hantavirus pulmonary syndrome, such as fever, chills, and aching. There is no treatment for hantavirus pulmonary syndrome, but receiving intubation, supplemental oxygen, and other supportive care can boost survival rates. The Yosemite cabins have been closed since August 28. The National Park Service is making changes to park facilities to help prevent future hantavirus outbreaks. Source: <http://www.latimes.com/health/boostershots/la-heb-hantavirus-yosemite-cdcupdate-20121121,0,6821344.story>

POSTAL AND SHIPPING

Mississippi River commerce imperiled by low water. A crucial 200-mile stretch of the Mississippi River may be on the verge of shutdown to barge traffic, a move that could paralyze commerce on a vital inland waterway and ultimately drive up consumer prices. The temporary closure of the Mississippi River from St. Louis to Cairo, Illinois, could result from an Army Corps of Engineers plan to reduce water flow from a reservoir into the Missouri River starting November 23, shipping companies and industry groups warned. The Corps annually decreases water releases to ensure adequate reservoir levels and to prevent ice buildup and flooding. In 2012, already-low river levels caused by drought could shrink to the point that barges carrying grain, coal, and other products would not be able to navigate the Mississippi, said a spokesperson with the Waterways Council, which represents ports and shippers. "This is an impending economic crisis that could delay shipment of \$7 billion in commodities in December and January," she said. A Corps spokeswoman said water releases from the reservoir at Gavins Point Dam on the Nebraska-South Dakota border will drop gradually starting November 23 from 36,000 cubic feet per second to 12,000 by December 11. Due to the drought, most vessels on the Mississippi River are now limited to a 9-foot draft, said a spokesperson with Knight Hawk Coal. "If we go to 6-foot drafts, the river is effectively closed," he said. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.firstcoastnews.com/news/usworld/article/283549/6/Mississippi-Rivercommerceimperiled-by-low-water>

PUBLIC HEALTH

Meningitis outbreak: FDA finds more contaminants in NECC meds. Testing by the U.S. Food and Drug Administration (FDA) on steroid medications produced by New England Compounding Center has found more contaminants in additional drugs, the Nashville Tennessean reported November 21. The FDA has updated its list of lot numbers for contaminated drugs after finding unknown fungal growths in triamcinolone and bethamethasone. It also found three forms of bacteria in betamethasone and one form of bacteria in trimacinolone. New England Compounding Center's products have been linked to a national outbreak of fungal meningitis and other infections that have sickened 490 people, with 34 deaths. Tennessee has had the most deaths with 13 and the second-most illnesses with 82. This is the first time that the FDA has confirmed contaminants in triamcinolone. However, the agency previously said in an inspection report that foreign substances were found on heating and cooling vent louvers behind a piece of equipment used to make bulk drug suspensions of preservative-free methylprednisolone and triamcinolone. Source:

http://www.tennessean.com/article/20121121/NEWS07/311210144/Meningitisoutbreak-FDAfindsmorecontaminantsNECCmeds?odyssey=mod|newswell|text|FRONTPAGE|p&gcheck=1&nlick_check=1

(Michigan) Mich.: 13 dead, 167 cases in meningitis outbreak. Officials said the Michigan death toll from a national meningitis outbreak rose to 13, with at least 167 infections reported. The Michigan Department of Community Health said November 21 that the State has had 67 cases of meningitis, including the 13 deaths. In addition, there have been 91 epidural abscesses, one stroke, and eight joint infections. The fungal meningitis is linked to contaminated steroids produced by a Massachusetts pharmacy used in injections for neck or back pain. Four deaths were from Livingston County and two from Washtenaw County, with one each in Cass, Charlevoix, Genesee, Ingham, and Wayne counties. Two other deaths involved Michigan residents infected in Indiana. Source:

<http://www.sturgisjournal.com/article/20121122/NEWS/121129888>

Indiana chickenpox outbreak largest in US, official says. The chief medical officer of the Indiana Department of Health said western Indiana's Vigo County is experiencing the largest known current outbreak of chickenpox in the U.S., the Associated Press reported November 23. The chief medical officer told the Terre Haute Tribune-Star that Vigo County usually has less than 10 cases per year. The county reported 84 cases since September. She said it is not clear why the county is having such a large outbreak. Vigo County School Corp. officials excluded 230 students from school the week of November 12 because of the outbreak. Source:

<http://www.foxnews.com/us/2012/11/23/indiana-chickenpox-outbreak-largest-in-us-official-says/>

UNCLASSIFIED

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

(Georgia) Major sewage spill caused by vandalism. More than 60,000 gallons of raw sewage spilled from a manhole over a two-day period the week of November 12 due to vandalism of Rockdale, Georgia's sewer system, according to Rockdale Water Resources (RWR). The RWR Deputy Director said it appeared that large rocks or boulders had been thrown into the manhole where the spill occurred or in a manhole upstream from the Scott Creek Wastewater Treatment Plant and then made their way down the sewer line. RWR was notified of the spill November 16 by a customer who called and said it appeared that sewage was overflowing from the manhole near a house. The deputy director said the spill flowed into a private pond on a nearby property. The department was notified of the spill and the sewer line problem was cleared the same day, stated Water Resources. The spill, which totaled 63,000 gallons, was classified as a major spill by the Georgia Environmental Protection Division (EPD). The deputy director said EPD had been notified that the spill was caused by vandalism, which could mean that only 12 months of monitoring of the spill site would be required. Source:

<http://www.rockdalecitizen.com/news/2012/nov/20/major-sewage-spill-caused-by-vandalism/>

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